

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'utilisateur dans la nouvelle loi sur les services de paiement

Bourguignon, Camille

Published in:
Actualités en droit du numérique

Publication date:
2019

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):
Bourguignon, C 2019, L'utilisateur dans la nouvelle loi sur les services de paiement: entre protection et responsabilisation. dans *Actualités en droit du numérique*. Recyclage en droit, numéro 2, Anthemis, Limal, pp. 153-215.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

L'utilisateur dans la nouvelle loi sur les services de paiement : entre protection et responsabilisation

Camille BOURGLIGNON¹

*Assistante à l'UNamur
Chercheuse au CRIDS-NaDI UNamur
Avocate au barreau de Paris*

Introduction

1. La nouvelle loi sur les services de paiement. – La loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique² (ci-après le « CDE ») est l'une des deux lois qui ont transposé en droit belge la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur³.

Ladite directive traite du secteur bien particulier des services de paiement.

2. Les services de paiement. – Quelque part entre les services financiers, les opérations bancaires et la monnaie électronique, les services de paiement renvoient à un ensemble d'activités dont les contours peuvent paraître techniques et bien abstraits. Pourtant, les services de paiement sont partout et utilisés de tous, et tous les jours. Ils recouvrent les achats par carte de crédit sur internet, le paiement de l'addition au restaurant par Bancontact, les opérations de virement bancaire, le retrait d'espèces à un distributeur automatique, le paiement sans contact, la domiciliation, etc. Des opérations qui nous concernent tous, donc.

Le législateur définit les services de paiement en en dressant une liste. Constituent, ainsi, des services de paiement : (i et ii) les services permettant de verser ou de retirer des espèces sur un compte de paiement, et toutes les opérations

¹ Avec nos remerciements vifs et sincères à Hervé Jacquemin pour la relecture de cette contribution et ses remarques éminemment pertinentes.

² M.B., 30 juillet 2018.

³ Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, J.O.U.E., L 337, 3 décembre 2015.

qu'exige la gestion d'un compte de paiement, (iii) l'exécution d'opérations de paiement, y compris les transferts de fonds sur un compte de paiement auprès du prestataire de services de paiement de l'utilisateur ou auprès d'un autre prestataire de services de paiement (prélèvements, opérations de paiement à l'aide d'une carte ou d'un autre dispositif, virements), (iv) l'exécution d'opérations de paiement dans le cadre desquelles les fonds sont couverts par une ligne de crédit accordée à l'utilisateur de services de paiement, (v) l'émission d'instruments de paiement et/ou l'acquisition d'opérations de paiement, (vi) les autres transmissions de fonds, (vii) les services d'initiation de paiement, ou encore (viii) les services d'information sur les comptes⁴.

3. Les deux directives sur les services de paiement. – La directive 2015/2366 concernant les services de paiement est souvent désignée par ses initiales accompagnées du chiffre 2. La « DSP 2 »⁵ donc (ou « PSD 2 » pour son équivalent anglais) arbore fièrement le chiffre 2 pour signifier qu'elle a eu un prédécesseur important dans l'encadrement, au niveau européen, des services de paiement.

4. La DSP 1. – Le 13 novembre 2007 était effectivement adoptée la première directive générale sur les services de paiement : la directive 2007/64, que l'on nomme désormais « DSP 1 » (ou « PSD 1 »)⁶. Partant du constat que les marchés des services de paiement étaient fragmentés, et les cadres réglementaires applicables essentiellement nationaux, malgré un certain nombre d'actes communautaires ponctuels adoptés dans le secteur⁷, il était alors considéré « crucial d'établir, au niveau communautaire, un cadre juridique moderne et cohérent pour les services de paiement »⁸. La DSP 1 a ainsi posé les bases de la réglementation générale sur les services de paiement. Elle s'était donné pour objectifs la coordination des dispositions nationales régissant les exigences prudentielles applicables aux prestataires de services de paiement, la garantie de l'accès au marché de nouveaux prestataires, la fixation d'exigences

⁴ Art. 4, 3), de la directive 2015/2366 concernant les services de paiement, renvoyant à son annexe I. Nous la nommerons également ainsi dans les présentes lignes.

⁵ Directive 2015/2366/CE du Parlement européen et du Conseil du 13 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, J.O.U.E., L 319, 5 décembre 2015 ; dans la présente étude, nous la nommerons « DSP 1 ».

⁷ En l'occurrence, le considérant n° 3 de la DSP 1 dresse, de ces actes, l'inventaire suivant : la directive 97/5/CE du Parlement européen et du Conseil du 27 janvier 1997 concernant les virements transfrontaliers, J.O.C.E., L 4, 14 décembre 1997 ; le règlement (CE) n° 2560/2001 du Parlement européen et du Conseil du 19 décembre 2001 concernant les paiements transfrontaliers en euros, J.O.C.E., L 344, 28 décembre 2001 ; la recommandation 87/598/CEE de la Commission du 8 décembre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique (relations entre institutions financières, commerçants-prestataires de services et consommateurs), J.O.C.E., L 365, 24 décembre 1987 ; la recommandation 88/590/CEE de la Commission du 17 novembre 1988 concernant les systèmes de paiement et en particulier les relations entre titulaires et émetteurs de cartes, J.O.C.E., L 317, 24 novembre 1988 ; la recommandation 97/489/CE de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, J.O.C.E., L 208, 2 août 1997.

⁸ Considérant n° 4 de la DSP 1.

d'information et la définition des droits et obligations des utilisateurs et des prestataires de services de paiement⁹.

La DSP 1 identifiait un ensemble d'acteurs considérés comme proposant des services de paiement et devant, à ce titre, endosser la qualification de « prestataires de services de paiement ». L'un des enjeux de la DSP 1 était d'encadrer les activités de ces prestataires en les soumettant, sauf dérogations¹⁰, à un certain nombre d'exigences (exigences prudentielles¹¹, et en particulier, pour les établissements de paiement¹² – catégorie de prestataires créée par la DSP 1 – obtention d'un agrément spécifique¹³, définition de droits et d'obligations particuliers¹⁴). L'on y trouvait les établissements de crédit, les établissements de monnaie électronique, les offices de chèques, les établissements de paiement, la Banque centrale européenne et les banques centrales nationales¹⁵ ou encore les États membres ou leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques¹⁶.

La DSP 1 a été transposée en droit belge par deux lois du 10 décembre 2009¹⁷ et du 21 décembre 2009¹⁸. La première encadrait les activités des services de paiement et prévoyait, notamment, les obligations des prestataires de services de paiement dans le cadre de leurs relations avec les utilisateurs. La seconde avait trait à l'encadrement de l'accès à l'activité de prestataires de services de paiement et aux règles prudentielles auxquelles ces derniers devaient se conformer¹⁹.

⁹ Voy. le considérant n° 5 de la DSP 1.

¹⁰ À côté des catégories de cette liste, pouvaient être qualifiées de prestataires de services de paiements également les personnes physiques ou morales fournissant des services de paiement bénéficiant d'une dérogation tel que prévu aux articles 26 et 27 de la DSP 1.

¹¹ Voy. le titre II de la DSP 1.

¹² L'établissement de paiement était défini, par l'article 4, 4), de la DSP 1, comme la « personne morale qui, conformément à l'article 10, a obtenu un agrément l'autorisant à fournir et à exécuter des services de paiement dans toute la Communauté ».

¹³ Pour l'agrément en tant qu'établissement de paiement, voy. les articles 5 et suivants de la DSP 1.

¹⁴ Voy. les titres III et IV de la DSP 1.

¹⁵ Lorsqu'elles n'agissent pas en qualité d'autorités monétaires ou autres autorités publiques.

¹⁶ Art. 4, 9), de la DSP 1 renvoyant à l'article 1^{er}, 1, de la même directive.

¹⁷ Loi du 10 décembre 2009 relative aux services de paiement, M.B., 15 janvier 2010. Cette loi a été abrogée, lors de la création du CDE, par la loi du 19 avril 2014 portant insertion du livre VII « Services de paiement et de crédit » dans le CDE, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres I et XV du CDE, et portant diverses autres dispositions, M.B., 28 mai 2014. Cette loi a, elle-même, été abrogée par la loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du CDE qui transpose la DSP 2 en droit belge.

¹⁸ Loi du 21 décembre 2009 relative au statut des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement, M.B., 19 janvier 2010. Cette loi a également été abrogée par la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, M.B., 26 mars 2018.

¹⁹ Pour un commentaire complet du cadre belge existant avant la transposition de la DSP 2, voy. notamment J. SAD, « Les services de paiement », in *Traité Pratique de Droit Commercial*, t. 5, Droit bancaire et financier, Waterloo, Kluwer, 2016, pp. 229-338.

5. La DSP 2. – La DSP 2 a été pensée et adoptée comme le prolongement de la directive qui lui a précédé. Il ne s'agissait pas de revoir de fond en comble le système mis en place par la DSP 1. Au contraire, il fallait partir de l'existant pour le réexaminer²⁰ et l'adapter aux nouveaux défis posés par l'innovation technique, l'apparition et la diversification des modes de paiement, et en particulier la croissance des paiements électroniques²¹. En d'autres mots, l'idée était de remettre le cadre applicable aux services de paiement au goût du jour²².

Dans cette optique, la DSP 2 a pris plusieurs directions²³.

6. Les directions prises par la DSP 2. – L'une de ses innovations majeures a été d'élargir son champ d'application à de nouveaux opérateurs. Ainsi, l'on voit apparaître de nouveaux acteurs réglementés en tant que prestataires de services de paiement : les prestataires de services d'initiation de paiement²⁴ ainsi que les prestataires de services d'information sur les comptes²⁵. La directive a également étendu le champ d'application de certaines de ces dispositions aux opérations de paiement effectuées en devises. Ainsi, sont désormais sous l'égide de la DSP 2, tant les opérations de paiement réalisées en euros que les opérations effectuées dans les devises des prestataires de services de paiement situés dans l'Union européenne, y compris lorsqu'un seul des prestataires engagés dans la transaction est situé au sein de l'Union²⁶. Un volet important de la DSP 2 est constitué également par le renforcement du rôle de l'Autorité bancaire européenne. Celle-ci est, en particulier, sollicitée

²⁰ Voy. en ce sens, T. BONNEAU, « La directive sur les services de paiement "2" : révolution ou évolution ? », *J.D.E.*, 2016/6, n° 230, pp. 214-217.

²¹ Voy. le considérant n° 3 de la DSP 2, selon lequel : « La directive 2007/64/CE a été adoptée en décembre 2007, sur la base d'une proposition présentée par la Commission en décembre 2005. Depuis lors, avec l'apparition de nouveaux types de services de paiement et la croissance rapide des paiements électroniques et mobiles, le marché des paiements de détail a connu d'importantes innovations techniques qui mettent à l'épreuve le cadre actuel. »

²² Ainsi, la DSP 2 reprend, dans son annexe I, la définition des services de paiement et, dans ses articles 4, 11) et 1^{er}, 1, l'identification des différents prestataires de paiements, d'ores et déjà développés dans la DSP 1. Elle crée deux nouveaux services de paiement identifiés qui sont les services d'initiation de paiement et les services d'information sur les comptes. Comme l'organisait la DSP 1, la DSP 2 soumet les prestataires de services de paiement à un ensemble de règles prudentielles définies, et les établissements de paiement à l'obtention d'un agrément spécifique (voy. à cet égard le titre II de la DSP 2) et leur reconnaît un ensemble de droits et d'obligations (voy. à cet égard les titres III et IV de la DSP 2).

²³ Pour des analyses détaillées de la DSP 2, voy. en particulier D. PHILIPPE, « La directive 2015/2366 sur les services de paiement (DSP 2) : la révolution digitale en marche », in *Actualités en droit commercial et bancaire*, Bruxelles, Larcier, 2017, pp. 455-477 ; T. BONNEAU, « La directive sur les services de paiement "2" : révolution ou évolution ? », *op. cit.*, pp. 214-217 ; T. BONNEAU, « Section IV. La protection des utilisateurs des services de paiement », in *Régulation bancaire et financière européenne et internationale*, Bruxelles, Bruylant, 2018, pp. 763-775.

²⁴ En vertu de l'article 4, 15), de la DSP 2, le service d'initiation de paiement désigne le « service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement ».

²⁵ En vertu de l'article 4, 16), de la DSP 2, le service d'information sur les comptes désigne le « service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement ».

²⁶ Art. 4 de la DSP 2.

dans le cadre de la mise en place de normes techniques en matière notamment d'authentification²⁷.

La DSP 2 tend, de manière générale, à renforcer la protection de l'utilisateur des services de paiement. Une mesure phare de la DSP 2 témoigne de cette tendance : la responsabilité de l'utilisateur en cas d'opérations de paiement non autorisées est désormais, sauf circonstances particulières, limitée à 50 euros, au lieu des 150 euros dans le régime précédent²⁸.

La DSP 2 devait être transposée dans les droits nationaux des États membres pour le 13 janvier 2018.

7. La transposition de la DSP 2 en droit belge. – En Belgique, comme pour la DSP 1, le législateur a procédé en deux temps. Tout d'abord, les volets prudentiels de la directive ont été transposés par la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement²⁹. Celle-ci est entrée en vigueur, à l'exception de certaines dispositions³⁰, le 28 mars 2018. Ensuite, en particulier pour ses volets « transparence et information » et « obligations du prestataire de services de paiement »³¹, la DSP 2 a été transposée par la loi du 19 juillet 2018 précitée qui a modifié, en particulier, le livre VII du CDE pour y insérer les modifications voulues par la directive³². Nous nous pencherons dans les développements qui suivent plus particulièrement sur les aspects abordés par cette seconde loi.

8. La transparence des services de paiement et la confiance des utilisateurs. – L'un des enjeux majeurs annoncés de la DSP 2 est de « renforcer l'efficacité du système de paiement dans son ensemble [, ce qui devrait] se traduire par un plus large choix et une plus grande transparence des services de paiement, ainsi que par une plus grande confiance des consommateurs à l'égard d'un marché des paiements harmonisé »³³. L'élargissement des possibilités de choix et le renforcement de la confiance des utilisateurs de services de paiement font ainsi partie des objectifs fondamentaux avoués de la DSP 2. La mise en œuvre de tels objectifs passera par une transparence toujours accrue de la part des prestataires de services de paiement et par une consolidation de la sécurité des services de paiement proposés.

²⁷ Sur ces normes techniques, voy. *infra*, section 2, § 2, A, 1.

²⁸ Art. 74 de la DSP 2 ; sur ce point, voy. *infra*, section 2, § 3, C, 2, a.

²⁹ M.B., 26 mars 2018.

³⁰ Sur ces exceptions, voy. *infra*, section 2, § 2, A, 1.

³¹ Qui nous intéresseront plus particulièrement dans le cadre de la présente contribution.

³² La transposition de la DSP 2 a été l'occasion, pour le législateur, de refondre entièrement les chapitres 2 à 7 du livre VII du CDE, en vue de coller davantage à la structure de la DSP 2. Sur ce point, voy. le projet de loi portant modification et insertion de dispositions en matière de services de paiement dans différents livres du CDE, exposé des motifs, *Doc.*, Ch., 2017-2018, n° 3131/001, p. 6.

³³ Considérant n° 6 de la DSP 2.

9. Champ de réflexion et plan de la présente étude. – Aussi, nous nous concentrerons dans cette étude sur la position et le rôle, voulus par la DSP 2, de l'utilisateur au sein du système des services de paiement. Nous verrons que deux tendances corollaires continuent de se dessiner et de se consolider : d'un côté, l'utilisateur bénéficie d'une protection accrue et, de l'autre, il est responsabilisé et joue un rôle actif dans la protection de ses instruments de paiement.

Nous constaterons ces deux tendances, qui s'accompagnent l'une l'autre, d'une part, au travers du renforcement de la transparence et des informations que le prestataire doit communiquer à l'utilisateur (section 1), d'autre part, dans la détermination des rôles que doivent jouer respectivement l'utilisateur et le prestataire de services de paiement en cas d'opérations de paiement non autorisées (section 2).

Section 1

La protection de l'utilisateur par un niveau égal et élevé d'information

10. Le renforcement de l'information de l'utilisateur. – La loi du 19 juillet 2018 précitée, comme la directive qu'elle transpose, confirme l'orientation prise dans la première directive sur les services de paiement : l'asymétrie d'informations entre le prestataire de services de paiement et l'utilisateur de ces services doit être compensée par une information renforcée au profit de l'utilisateur. Le législateur donne précisément la marche à suivre pour parvenir à une telle compensation.

En matière de services de paiements, le législateur a, d'une part, dressé la liste détaillée des informations minimales que doit recevoir l'utilisateur d'un service de paiement et, d'autre part, précisé les modalités selon lesquelles ces informations doivent être communiquées à l'utilisateur. L'objectif *in fine* pour l'utilisateur est de disposer d'un niveau d'information qui soit uniforme et élevé, quel que soit l'opérateur qu'il sollicite au sein de l'Union européenne.

§ 1. La *ratio legis* inchangée : un niveau égal et élevé d'information permettant un choix éclairé

11. Un niveau égal et élevé d'information dans toute l'Union européenne. – La matière des services de paiement s'inscrit dans une tendance législative européenne d'intervention poussée du législateur, ne laissant *in fine* que très peu de marge d'appréciation aux États membres transposant le texte européen et aux opérateurs l'appliquant. L'objectif est la mise en place d'un niveau uniformisé et élevé d'information visant à compenser l'asymétrie d'informations postulée entre les parties intervenantes³⁴.

³⁴ Sur cette notion d'asymétrie d'informations, voy. en particulier H. JACQUEMIN, « Le formalisme de protection de la partie faible au rapport contractuel », *Ann. dr.*, 2010/1, pp. 11 et s.

Un autre exemple emblématique de cette tendance est le droit du commerce électronique, et plus spécifiquement les contrats à distance³⁵.

12. Le postulat de l'asymétrie d'information entre l'utilisateur et le prestataire de services de paiement. – On comprend aisément qu'une personne, en particulier une personne physique, n'intervenant pas dans le champ d'une quelconque expertise professionnelle, ne sera pas sur un pied d'égalité face à une entreprise, fournisseur de biens et/ou de services, dont le métier – et l'objectif – est de convaincre des clients potentiels et de conclure avec ceux-ci des contrats. Asymétrie d'information, mais également raison d'être initiale de l'entreprise (la recherche de clients et la conclusion de contrats), font que le cocontractant, non professionnel du moins, sera en situation de faiblesse à son égard³⁶.

Partant de ce postulat, le législateur a jugé que la personne physique non professionnelle, considérée comme partie « faible » au contrat – en droit du commerce électronique, et de manière plus générale en droit de la consommation, l'on parlera du « consommateur »³⁷ – doit être protégée. Cette protection passe par une information renforcée, de sorte que ladite personne puisse se décider en faveur de tel opérateur, de tel bien, de tel service, sur la base d'un certain nombre d'informations qui lui permettent d'accepter ou non de contracter et, si elle opte pour la première hypothèse, d'opérer un choix parmi les différentes possibilités apparaissant, grâce à ces informations, à ses yeux à tout le moins, équivalentes et concurrentes pour répondre à son besoin spécifique. Le but est ainsi de corriger, de manière forcée, le déficit supposé d'informations initial pour aboutir *in fine* à un choix éclairé par la personne concernée.

C'est cette optique qui a été poursuivie par le législateur européen dans la première directive sur les services de paiements³⁸. Elle est confirmée et renforcée dans la DSP 2. Reprenant l'explication développée dans la première directive, la DSP 2 fixe en effet « les obligations incombant aux prestataires de services de paiement [...], lesquels, pour pouvoir faire un choix éclairé et être en mesure de choisir librement dans toute l'Union, devraient recevoir des informations claires, d'un niveau partout égal et élevé »³⁹.

³⁵ Voy. à cet égard le livre VI du CDE qui dresse la liste détaillée des informations minimales à fournir par l'entreprise proposant ses biens, services et/ou contenus numériques au consommateur lorsqu'est envisagée la conclusion d'un contrat à distance ne portant pas sur des services financiers (art. VI.45) et portant sur des services financiers (art. VI.55), et indique les modalités précises de fourniture de ces informations.

³⁶ Sur la faiblesse d'une des parties au contrat, voy. H. JACQUEMIN, « Chapitre 8 – Protection du Consommateur et numérique en droits européen et belge », in *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 240 et s. ; H. JACQUEMIN, « Heurs et malheurs du formalisme contractuel comme mécanisme de protection du consommateur », *D.C.C.R.*, 2013/3-4, n° 100, pp. 267-286 ; H. JACQUEMIN, « Le formalisme de protection de la partie faible au rapport contractuel », *op. cit.*, pp. 8 et s. ; sur la faiblesse du consommateur en matière de services de paiement, voy. H. JACQUEMIN, « Les paiements électroniques dans les contrats à distance depuis la loi du 10 décembre 2009 », *R.D.T.I.*, 2010/4, n° 41, pp. 9 et 10.

³⁷ Voy. l'article 1.1, 2°, du CDE, selon lequel le consommateur désigne « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ».

³⁸ Voy. en ce sens, le considérant n° 21 de la DSP 1.

³⁹ Considérant n° 54 de la DSP 2.

13. Une harmonisation européenne « totale ». – Le législateur européen précise que le bon fonctionnement du marché intérieur implique que « les États membres n'adoptent pas de dispositions en matière d'information différentes de celles établies par la présente directive »⁴⁰. Il insiste sur ce point et fait de la DSP 2 une directive d'« harmonisation totale »⁴¹. À ce titre, « les États membres ne peuvent maintenir en vigueur ni introduire des dispositions différentes de celles contenues dans la présente directive »⁴². La marge de manœuvre de la Belgique dans la transposition de la DSP 2, au regard de l'obligation d'information, était donc très faible⁴³.

14. Informations. – Ainsi, le chapitre 2 du livre VII du CDE, issu de la loi du 19 juillet 2018 précitée, est consacré, comme son titre l'indique, aux « Informations et conditions régissant les opérations et les contrats-cadre ».

§ 2. Une obligation d'information au bénéfice de l'utilisateur

15. La notion d'utilisateur de services de paiement. – L'information, dont le prestataire de services de paiement est débiteur, devra bénéficier, et donc être communiquée, à l'utilisateur de ses services.

L'utilisateur de services de paiement est « la personne physique ou morale qui utilise un service de paiement en qualité de payeur, de bénéficiaire ou les deux »⁴⁴.

Nous constatons d'emblée que la notion d'utilisateur couvre tant l'utilisateur qui intervient en tant que payeur⁴⁵ dans le cadre de l'opération de paiement envisagée que celui qui intervient en tant que bénéficiaire⁴⁶ de l'opération.

La définition d'« utilisateur de services de paiement » est également indifférente à l'éventuel statut de consommateur⁴⁷, ou de non-consommateur, dudit

⁴⁰ *Ibid.*

⁴¹ Art. 107 de la DSP 2.

⁴² Art. 107, § 1^{er}, de la DSP 2.

⁴³ Ce qui était d'ailleurs déjà le cas lors de la transposition de la DSP 1 ; outre certaines reformulations du texte ou de certaines expressions (par exemple, l'article VII.41, § 1^{er}, du CDE prévoit que le prestataire ne corrigera une opération de paiement non autorisée ou mal exécutée que si l'utilisateur l'en a informé « sans délai », au lieu de « sans retard injustifié » dans l'article 71, § 1^{er}, de la DSP 2), le législateur belge a transposé, pour une très large partie à la lettre, la DSP 2. Il a toutefois maintenu certains textes spécifiques à la législation belge. On notera notamment l'article VII.33 qui a trait à la domiciliation et qui n'est pas issu de la DSP 2, ou encore l'obligation d'ajouter, le cas échéant, aux obligations à fournir dans le cas d'un contrat-cadre des informations particulières concernant le contrat de crédit, prévue par l'article VII.21, § 3, alinéa 2, du CDE.

⁴⁴ Art. 1.9, 3^o, du CDE.

⁴⁵ En vertu de l'article 1.9, 4^o, du CDE, le payeur désigne « la personne physique ou morale qui est titulaire d'un compte de paiement et qui autorise un ordre de paiement à partir de ce compte de paiement, ou, la personne physique ou morale qui, en l'absence de compte de paiement, donne un ordre de paiement ».

⁴⁶ En vertu de l'article 1.9, 5^o, du CDE, le bénéficiaire désigne « la personne physique ou morale qui est le destinataire prévu de fonds ayant fait l'objet d'une opération de paiement ».

⁴⁷ La notion de consommateur est définie de manière spécifique dans la DSP 2. Son article 4, 20^o, fait du consommateur la « personne physique qui, dans le cadre des contrats de services de paiement régis par la présente directive, agit dans un but autre que son activité commerciale ou professionnelle ». Une telle définition est reprise telle quelle de la première directive. Le CDE est moins précis. Il se contente, effectivement, de se référer, comme avant la transposition, à la définition générale du « consommateur » consacrée à l'article 1.1, 2^o, du Code, qui s'applique à l'ensemble des livres du Code, sauf clause contraire. Cette définition, qui fait

utilisateur. Nous verrons toutefois qu'au regard de l'obligation d'information pesant sur le prestataire de services de paiement, le statut de l'utilisateur (consommateur ou non) a un impact crucial. Le caractère contraignant de l'obligation d'information ne sera en effet pas le même selon que l'utilisateur sera un consommateur ou un non-consommateur⁴⁸.

16. Le caractère contraignant variable de l'obligation d'information selon que l'utilisateur est un consommateur ou non. – Les obligations en matière de transparence et d'information revêtent un caractère impératif à l'égard de l'utilisateur consommateur. Autrement dit, il ne peut y être dérogé contractuellement. À l'inverse, le législateur permet aux parties, lorsque l'utilisateur n'est pas un consommateur, de déroger par contrat à ces obligations de transparence et d'information⁴⁹. À l'égard de l'utilisateur non consommateur, lesdites obligations n'ont, à ce titre, qu'un caractère supplétif⁵⁰.

17. Comparaison avec le droit des contrats à distance. – La comparaison, ici, avec le droit des contrats à distance⁵¹ est intéressante. En effet, on constate que le non-consommateur en matière de services de paiement se trouve davantage protégé qu'il ne l'est en matière de contrat à distance.

du consommateur « la personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, artisanale, industrielle ou libérale », est ainsi plus large que celle consacrée dans la directive, en ce qu'elle ne se réfère pas précisément aux contrats de services de paiement. Une telle nuance ne nous semble toutefois pas susceptible d'avoir un impact en pratique.

⁴⁸ Voy. le considérant n° 53 de la DSP 2 selon lequel : « Ne se trouvant pas dans la même situation, consommateur et entreprise n'ont pas besoin du même niveau de protection. »

⁴⁹ La règle était posée à l'article VII.26 du CDE, elle est désormais reprise telle quelle au nouvel article VII.5 du même Code. On y lit que : « Les parties peuvent convenir de ne pas appliquer, en tout ou en partie, les dispositions du présent chapitre [consacré aux « Informations et conditions régissant les opérations de paiement et les contrats-cadre »], sauf si l'utilisateur des services de paiement est un consommateur ». Il est à noter que le législateur belge a pris une légère liberté quant à la formulation du principe : l'article VII.5 semble en effet suggérer, à tort selon nous, que l'obligation d'information ne s'appliquerait que dans le cas – qui n'aurait à la lecture de l'article de la loi belge qu'un caractère exceptionnel – où le contrat est envisagé avec un consommateur. Néanmoins, il ne peut être, ainsi, suggéré qu'une telle situation est exceptionnelle. Ce serait faire fi de la réalité. Il est par ailleurs étonnant de reléguer ainsi à la position d'exception un principe, celui d'une obligation d'information renforcée, qui est pourtant présenté comme à la base de la DSP 2 et appuyé à ce titre dans l'un de ses considérants (son considérant 54). La formulation de la directive est à cet égard bien plus appropriée. Le législateur européen s'est effectivement montré plus neutre : il s'est contenté d'indiquer, en mettant sur le même plan les deux situations, que « lorsque l'utilisateur de services de paiement n'est pas un consommateur », « les parties peuvent décider de ne pas [appliquer le présent titre consacré à la transparence et les exigences en matière d'informations] » (art. 38, § 1^{er}, de la DSP 2). Il aurait été plus sage de conserver une telle formulation. Si le texte belge, *in fine*, n'aura certainement pas d'impact pratique, et n'en a pas eu jusqu'à ce jour à notre connaissance, il tend à ternir le principe mis en avant de l'obligation d'informations renforcée, ce qui, selon nous, n'est pas heureux.

⁵⁰ Voy. en ce sens, J. SAD, « Les services de paiement », *op. cit.*, n° 360, p. 267.

⁵¹ En vertu de l'article 1.8, 15^o, du CDE, le contrat à distance désigne : « tout contrat conclu entre l'entreprise et le consommateur, dans le cadre d'un système organisé de vente ou de prestation de service à distance, sans la présence physique simultanée de l'entreprise et du consommateur, par le recours exclusif à une ou plusieurs techniques de communication à distance, jusqu'au moment, et y compris au moment, où le contrat est conclu ». Le contrat à distance renvoie au contrat qui serait conclu en ligne, par téléphone ou par fax, par exemple. Pour faciliter l'analyse, il ne sera fait référence ici qu'au contrat à distance ne portant pas sur des services financiers, encadré par les articles VI.44/1 à VI.53 du CDE.

Dans le cas d'un contrat à distance, l'obligation d'information précontractuelle pesant sur l'entreprise⁵² s'applique, de manière impérative, lorsque le cocontractant est un consommateur. Jusqu'ici, il n'y a pas de différence avec les services de paiement. Une telle obligation, en revanche, ne s'applique pas au contrat à distance, lorsque le cocontractant n'est pas un consommateur. Elle ne s'impose tout simplement pas à l'entreprise, sans que cette dernière n'ait à y déroger, d'une quelconque manière, par contrat. À l'inverse, et là se situe la différence, le prestataire de services de paiement qui contracte avec un utilisateur non consommateur devra faire l'effort de déroger, par contrat, à l'obligation légale d'information ; à défaut, il y sera soumis.

18. La forme de la dérogation. – La loi n'implique pas pour autant qu'une telle dérogation à l'obligation d'information soit expressément formulée dans le contrat. Le fait pour le prestataire de ne pas communiquer lesdites informations, selon les modalités imposées par la loi, peut ainsi suffire à extérioriser la volonté du prestataire de ne pas soumettre le contrat à ladite obligation d'information, et donc d'y déroger. On pourra considérer que le non-consommateur qui, malgré ce défaut de communication d'informations, contracte avec le prestataire, sera réputé accepter, implicitement, la dérogation voulue par le prestataire.

Toutefois, l'on s'interroge : ne serait-il pas plus prudent, pour le prestataire de services de paiement, d'exprimer expressément dans le contrat avec l'utilisateur non consommateur sa volonté de déroger à tout ou partie de l'obligation légale d'information ? En effet, l'utilisateur pourrait contester sa propre volonté d'accepter une telle dérogation. La preuve de l'acceptation d'une telle dérogation par le cocontractant sera difficile, voire impossible, à apporter. En toute hypothèse, il est certain qu'une dérogation expresse serait admise au regard de la loi⁵³ et aurait l'avantage d'ôter tout doute à l'utilisateur non consommateur quant au droit qui lui est applicable ou non.

19. L'exclusion des microentreprises du caractère impératif de l'obligation d'information. – La Belgique a confirmé le choix qu'elle avait opéré dès la transposition de la première directive de ne pas étendre le régime protecteur prévu pour les consommateurs aux microentreprises. La DSP 2 laissait aux États la possibilité d'appliquer les dispositions protectrices en matière d'information aux microentreprises⁵⁴ « de la même manière qu'aux consommateurs »⁵⁵, c'est-à-dire en leur conférant un caractère impératif.

⁵² Prévue à l'article VI.45 du CDE.

⁵³ Voy. en ce sens, J. SAD, « Les services de paiement », *op. cit.*, n° 360, p. 267.

⁵⁴ La microentreprise désigne, conformément à l'article 4, 36°, de la DSP 2, l'entreprise qui, au moment de la conclusion du contrat de service de paiement, est une « entreprise au sens de l'article 1^{er} et de l'article 2, paragraphes 1 et 3, de l'annexe de la recommandation 2003/361/CE » de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (J.O.U.E., L 124, 20 mai 2003). Il s'agit donc de « toute entité, indépendamment de sa forme juridique, exerçant une activité économique. Sont notamment considérées comme telles les entités exerçant une activité artisanale ou d'autres activités à titre individuel ou familial, les sociétés de personnes ou les associations qui exercent régulièrement une activité économique », occupant « moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros ».

⁵⁵ Art. 38, § 2, de la DSP 2.

Le but pour le législateur belge, en n'étendant pas ce régime protecteur aux microentreprises, a été de « laisser un régime plus souple à l'égard des non-consommateurs notamment entre commerçants »⁵⁶. Il n'est toutefois pas certain que ce choix soit judicieux, dès lors que nous supposons qu'une microentreprise, non professionnelle des paiements, sera rarement en mesure de bénéficier d'une telle souplesse⁵⁷. La question précédemment évoquée du caractère exprès ou non de la dérogation contractuelle à l'obligation légale d'information prend ici une acuité toute particulière : un juge pourra-t-il considérer qu'une microentreprise n'ayant aucune expertise dans les paiements ni aucune connaissance particulière de la législation, somme toute assez technique, qui s'y applique, puisse être réputée ayant accepté implicitement une dérogation dont elle n'est, dans les faits, probablement pas en mesure de connaître les conséquences ni même l'existence ? Rien n'est moins sûr. Le caractère exprès de la dérogation devra donc, selon nous, être considéré, au moins lorsque le cocontractant est une microentreprise.

§ 3. Le contenu de l'obligation d'information renforcé

A. Un contenu variable selon les opérations de paiement

20. Les différentes catégories d'opérations de paiement. – L'opération de paiement désigne « une action, initiée par le payeur ou [pour son compte ou] par le bénéficiaire, consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire »⁵⁸. Ladite opération de paiement peut être entreprise soit en

⁵⁶ Projet de loi n° 3131/001 précité, p. 22 ; voy. également le projet de loi relatif aux services de paiement, exposé des motifs, *Doc.*, Ch., 2008-2009, n° 2179/001, p. 34.

⁵⁷ Insérer ainsi, sans établir aucune distinction, les microentreprises dans la catégorie plus générale de l'« entreprise », en opposition notamment aux consommateurs, nous semble participer de l'approche englobante voulue par le législateur. Par la loi du 15 avril 2018 portant réforme du droit des entreprises (M.B., 27 avril 2018), le législateur belge a redéfini la notion d'entreprise en lui consacrant, à l'article 1.1, du CDE, une nouvelle définition. L'entreprise désigne désormais « chacune des organisations suivantes : (a) toute personne physique qui exerce une activité professionnelle à titre indépendant ; (b) toute personne morale ; (c) toute autre organisation sans personnalité juridique ». Le législateur a notamment supprimé la notion de « commerçant » et intégré, par ailleurs, dans la notion globale d'entreprise, les professions libérales. Les commentateurs indiquent que le législateur est ainsi passé d'une définition « fonctionnelle » de l'entreprise, qui mettait l'accent sur l'objet de l'activité de la personne en ce qu'elle devait poursuivre un « but économique », à une définition davantage « formelle » liée au statut ou à l'organisation de la personne en question ; voy. en ce sens, H. CULOT, Y. DE CORDT, H. JACQUEMIN et Th. LÉONARD, *Manuel du droit de l'entreprise*, Limal, Anthemis, 2019, pp. 46-47, n° 58 ; on pourra craindre que cette tendance à englober diverses formes d'acteurs économiques dans une seule et même notion d'entreprise, en mettant l'accent essentiellement sur leur statut, n'ait pour conséquence de cacher des différences majeures entre ces acteurs, qui résideraient par exemple dans leur différence de taille, et qui impliqueraient pourtant une différenciation du cadre juridique applicable, ou, le cas échéant, davantage de protection. De la même manière, en matière de services de paiement, englober les microentreprises dans la notion plus globale d'entreprise tendra à ne pas tenir compte de la situation propre de ces microentreprises, qui tient à leur taille et à leur poids économique, les plaçant, dans la majorité des cas, dans une situation d'impossibilité factuelle de négocier face à un acteur économique dont l'expertise et le poids économique seront en général plus importants.

⁵⁸ Art. 1.9, 6°, du CDE. Cette définition a été modifiée par la nouvelle loi du 19 juillet 2018 pour y insérer l'idée que l'opération de paiement peut être initiée par le bénéficiaire du paiement et par le payeur, mais également,

vertu d'un contrat-cadre, à savoir d'un « contrat de services de paiement qui régit l'exécution future d'opérations de paiement particulières et successives [...] »⁵⁹, soit de manière isolée, hors de tout contrat-cadre. Partant, le CDE distingue d'une part, les opérations de paiement isolées, et d'autre part, les contrats-cadre et les opérations de paiement individuelles couvertes par ceux-ci. Le contenu et l'étendue de l'obligation d'information seront plus ou moins importants selon le service de paiement envisagé⁶⁰.

Une telle distinction, entre l'opération de paiement isolée et le contrat-cadre, dans le contenu des informations à communiquer s'explique par le fait que les opérations de paiement isolées et les opérations de paiement couvertes par un contrat-cadre n'ont pas le même impact économique ni la même fréquence, les premières étant beaucoup plus rares⁶¹. Les informations que doit recevoir l'utilisateur doivent, à ce titre, être adaptées au niveau de leur contenu, comme au niveau des modalités de leur communication^{62,63}. Les informations à communiquer dans le cas d'opérations de paiement isolées sont, à cet égard, allégées.

1. Le contenu de l'obligation d'information en cas d'opérations de paiement isolées

21. La notion d'opération de paiement isolée. – Le législateur précise que les opérations de paiement isolées visent « notamment un type particulier de pratiques commerciales anglo-saxonnes, comme les transmissions de fonds⁶⁴ (“*Money remittance*”), et certains modèles de services de paiement de factures (“*bill payment services*”) »⁶⁵.

et il s'agit là de l'ajout apporté, pour le compte de ce payeur. Une erreur matérielle semble s'être glissée, dans le texte *in fine* inséré à l'article 1.9, 6°, du CDE, qui définit l'opération de paiement comme « l'action, initiée par le payeur ou [par le payeur ou] le bénéficiaire, consistant [...] ». L'expression entre crochets dans le code aurait dû contenir, en vertu de l'article 2, 4°, de la loi du 19 juillet 2018, l'expression [pour son compte ou par].

⁵⁹ Art. 1.9, 16°, du CDE.

⁶⁰ L'obligation d'information relative aux opérations de paiement isolées est désormais détaillée dans les articles VII.12 à VII.19, et l'obligation d'information concernant les contrats-cadre, et les opérations individuelles qu'ils couvrent, fait l'objet des nouveaux articles VII.20 à VII.28. Outre une numérotation nouvelle, l'essentiel des modifications apportées par la loi de transposition de la DSP 2 a trait aux informations à fournir, ou à mettre à disposition, lorsqu'intervient un prestataire de services d'initiation de paiement, catégorie de prestataires de services de paiement nouvellement créée et réglementée par la DSP 2.

⁶¹ Projet de loi n° 3131/001 précité, p. 25.

⁶² *Ibid.* ; voy. également le considérant n° 56 de la DSP 2.

⁶³ La communication des informations prendra la forme, selon les cas, soit d'une *fourniture*, soit d'une *mise à disposition*. Pour faciliter la lecture des paragraphes 3 et 4 de la section 1, nous emploierons, néanmoins, le mot *communication*, décliné le cas échéant en verbe, conjugué ou non, pour désigner indifféremment la *fourniture* ou la *mise à disposition*, sauf lorsqu'une distinction entre les deux notions est nécessaire. Sur la distinction de ces deux modalités de communication de l'information voy. *infra*, section 1, § 4, C.

⁶⁴ La transmission de fonds désigne, en vertu de l'article 1.9, 14°, du CDE, « un service de paiement par lequel les fonds sont reçus de la part d'un payeur, sans création de comptes de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant correspondant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, et/ou par lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci ». Il s'agira, par exemple, des services de transfert de fonds proposés par Western Union.

⁶⁵ Projet de loi n° 2179/001 précité, p. 34 ; les mêmes exemples sont repris dans le projet de loi n° 3131/001 précité, p. 25.

22. Les informations à communiquer en cas d'opérations de paiement isolées. – Le prestataire de services de paiement doit communiquer un certain nombre d'informations à deux moments précis de l'opération de paiement isolée : (1) avant que l'utilisateur de service de paiement ne soit lié par un contrat ou une offre de services de paiement isolé, et (2) après que l'ordre de paiement a été initié ou reçu et que la transaction a été exécutée.

Ainsi, le prestataire doit communiquer à l'utilisateur, avant que celui-ci ne soit lié par un contrat ou une offre, un certain nombre d'informations concernant l'opération de paiement envisagée⁶⁶. En cas d'opérations de paiement initiées par le biais d'un prestataire de services d'initiation de paiement, celui-ci devra communiquer des informations ayant trait à son identification⁶⁷, son enregistrement, ainsi qu'à l'autorité de régulation dont il relève⁶⁸.

Après qu'un ordre de paiement a été initié ou reçu et que la transaction a été exécutée, l'utilisateur doit se voir communiquer un ensemble d'informations sur l'opération qui vient d'être exécutée⁶⁹. Ainsi, le prestataire de services de paiement du payeur communiquera à celui-ci les informations lui permettant d'identifier l'opération de paiement en question, son montant, le montant des frais imputables, le cas échéant, le taux de change applicable, ainsi que la date de réception de l'ordre de paiement. Le bénéficiaire de l'opération de paiement reçoit de son prestataire le même type d'informations. Dans le cas où l'ordre de paiement a été initié par un prestataire de services d'initiation de paiement, celui-ci doit également communiquer à l'utilisateur payeur, et le cas échéant, à l'utilisateur bénéficiaire, un certain nombre d'informations ayant trait à l'opération qui vient d'être effectuée⁷⁰.

⁶⁶ Le prestataire doit, en vertu de l'article VII.15, § 1°, du CDE, communiquer, au minimum : (1) des informations précises ou l'identifiant unique que l'utilisateur doit fournir aux fins de l'initiation ou de l'exécution correcte de son ordre de paiement, (2) le délai d'exécution maximal de fourniture du service de paiement, (3) les frais à la charge de l'utilisateur à payer à son prestataire de services de paiement ou, le cas échéant, leur ventilation, et enfin (4) le cas échéant, le taux de change réel ou de référence devant être appliqué à l'opération de paiement.

⁶⁷ En vertu de l'article VII.15, § 2, 1°, du CDE, le prestataire de services d'initiation de paiement doit ainsi communiquer son identité, « son numéro d'entreprise, l'adresse géographique de son administration centrale, le cas échéant, l'adresse géographique de son agent ou de sa succursale établi en Belgique, dans lequel le service de paiement est proposé, et toutes les autres coordonnées, y compris l'adresse de courrier électronique, à prendre en compte pour la communication avec le prestataire de services d'initiation de paiement ».

⁶⁸ En vertu de l'article VII.15, § 2, 2°, du CDE, le prestataire fournit ou met à disposition « les coordonnées de l'autorité de contrôle prudentielle compétence et le registre concerné auprès de cette autorité dans lequel le prestataire de services d'initiation de paiement est inscrit en vue de son agrément, ainsi que son numéro d'enregistrement ou un moyen équivalent d'identification de ce registre ».

⁶⁹ Les articles VII.18 et VII.19 du CDE reprennent en substance les anciens articles VII. 9 et VII.10, sans que le contenu des informations à communiquer n'ait été modifié.

⁷⁰ En vertu du nouvel article VII.16 du CDE, il s'agira de la confirmation de la réussite de l'initiation de paiement, de la référence permettant d'identifier l'opération de paiement, du montant de ladite opération, et le cas échéant, du montant des frais payables au prestataire de services d'initiation de paiement. En vertu du nouvel article VII.17 du CDE, le prestataire de services d'initiation de paiement est également tenu de mettre à la disposition du prestataire gestionnaire du compte du payeur la référence de l'opération de paiement.

2. *Le contenu de l'obligation d'information en cas de contrat-cadre ou d'opérations de paiement individuelles couvertes par un contrat-cadre*

23. La notion de contrat-cadre et les opérations qu'il couvre. – Par la notion de contrat-cadre, le législateur désigne le « contrat de services de paiement qui régit l'exécution future d'opérations de paiement particulières et successives et peut énoncer les obligations et les conditions liées à l'ouverture d'un compte de paiement »⁷¹. Le législateur précise qu'« il s'agit par exemple d'un contrat de gestion d'un compte de paiement ou de mise à disposition et d'utilisation d'un instrument de paiement. De tels contrats comportent différentes opérations, comme le dépôt ou le retrait d'argent sur le compte, l'exécution d'opération avec l'instrument, etc. »⁷². Le contrat-cadre pourra organiser des opérations aussi diverses que quotidiennes pour l'utilisateur, comme l'ouverture d'un compte bancaire, les virements mensuels à réaliser pour le paiement de loyers locatifs via son *home-banking*, la domiciliation à mettre en place pour le règlement des cotisations permettant l'accès à sa salle de sport, etc. Le contrat-cadre prendra, par exemple, la forme d'un règlement général des opérations ou de conditions bancaires générales.

Les contrats-cadre et les opérations qui sont réalisées en vertu de ces contrats sont considérés comme beaucoup plus fréquents et d'une importance économique beaucoup plus grande que les opérations de paiement isolés⁷³. Par conséquent, les obligations d'information au regard de ces contrats-cadres sont « beaucoup plus globales et dans certains cas beaucoup plus sévères »⁷⁴.

a) *Les informations générales relatives au contrat-cadre*

24. Présentation générale. – Le législateur liste de manière détaillée les différentes informations devant être communiquées à l'utilisateur de services de paiement, en prenant le soin de les présenter par catégorie⁷⁵. Une telle présentation a le mérite de rendre la disposition légale lisible et claire, et permet au prestataire de vérifier que les informations qu'il communique à ses utilisateurs sont suffisantes pour se conformer au prescrit légal.

Sept catégories d'informations sont ainsi identifiées⁷⁶. Elles seront développées l'une après l'autre ci-dessous.

⁷¹ Art. 1.8, 16°, du CDE.

⁷² Projet de loi n° 3131/001 précité, p. 29.

⁷³ *Ibid.* ; considérant n° 27 de la DSP 2.

⁷⁴ Projet de loi n° 3131/001 précité, p. 29.

⁷⁵ Ladite liste se retrouve à l'article VII.22 du CDE, qui reprend, pour une grande partie, l'ancien article VII.13 et transpose certains points nouveaux développés par l'article 52 de la DSP 2.

⁷⁶ Les sept catégories d'informations ainsi identifiées sont les suivantes : les informations relatives (1) au prestataire de services de paiement, (2) à l'utilisation d'un service de paiement, (3) aux frais, aux taux d'intérêt et aux taux de change, (4) aux modalités de communication entre le prestataire et l'utilisateur de services de paiement pendant l'exécution du contrat-cadre, (5) aux mesures de protection et aux mesures correctrices à mettre en œuvre par le prestataire et par l'utilisateur en vue d'assurer la sécurité d'un instrument de paiement et, de manière générale, de prévenir ou corriger la fraude, (6) à la modification et la résiliation du contrat, et enfin (7) aux recours pouvant être mis en œuvre en cas de litiges entre le prestataire et l'utilisateur.

25. Informations sur le prestataire de services de paiement (art. VII.22, 1°, du CDE). – Tout d'abord, le prestataire doit communiquer son identité, en ce compris son numéro d'entreprise, son adresse géographique, le cas échéant, celle de son agent ou de sa succursale, ainsi que toutes les autres coordonnées à prendre en compte pour la communication avec l'utilisateur.

À l'égard de ces « autres coordonnées », l'article VII.22, 1°, a), du CDE se réfère expressément à l'adresse électronique du prestataire en en faisant le moyen de contact à indiquer au minimum, parmi d'autres moyens de communication possibles. La disposition se lit comme suit : « toutes les autres coordonnées, y compris l'adresse du courrier électronique ».

À la lecture de la jurisprudence de la Cour de justice de l'Union européenne, la communication des seules adresses géographique et électronique ne suffira pas à remplir l'exigence prescrite en matière d'information. Le prestataire devra indiquer un autre moyen de communication.

La Cour de justice a en effet été interrogée sur le point de savoir si un prestataire – en l'espèce, il ne s'agissait pas d'un prestataire de services de paiement mais d'un prestataire de services de la société de l'information – devait, en plus de son adresse électronique, indiquer nécessairement un numéro de téléphone⁷⁷. Le cadre applicable alors était la directive 2000/31 relative au commerce électronique⁷⁸, et précisément son article 5, § 1^{er}, c), qui oblige le prestataire à fournir ses coordonnées « y compris son adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec lui ». La Cour de justice a d'abord confirmé que l'adresse électronique était un strict minimum, en ce sens que d'autres coordonnées de contact devaient être communiquées. Pour la Cour, il ressort en effet « de la locution “y compris” que le législateur communautaire a entendu exiger du prestataire de services qu'il fournisse aux destinataires du service, outre son adresse de courrier électronique, d'autres informations permettant d'atteindre le résultat visé par cette disposition »⁷⁹. La même locution étant utilisée dans l'article VII.22, 1°, a), il doit être considéré que le prestataire de services de paiement devra également fournir, outre son adresse électronique et son adresse géographique, d'autres moyens permettant de communiquer avec lui.

Quelles sont donc les autres coordonnées à fournir par le prestataire si l'adresse électronique et son adresse géographique ne suffisent pas ? L'on pourrait estimer que le prestataire est libre d'en décider. La Cour de justice, dans l'arrêt précité, semble se montrer souple quant à l'autre moyen de communication

⁷⁷ C.J., arrêt *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. deutsche internet versicherung AG*, 16 octobre 2008, C-298/07, EU:C:2008:572.

⁷⁸ Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), J.O.C.E., L 178, 17 juillet 2000.

⁷⁹ C.J., arrêt *deutsche internet versicherung*, 16 octobre 2008, C-298/07, point 17.

que le prestataire doit indiquer, en ce que cet autre moyen ne devrait pas être nécessairement un numéro de téléphone⁸⁰. L'avocat général à la Cour de justice Giovanni Pitruzzella a confirmé, dans ses conclusions déposées le 28 février 2019, une telle position. Il se prononçait alors sur l'article 6, § 1^{er}, c), de la directive 2011/83/UE sur le droit des consommateurs⁸¹, qui exige du professionnel proposant un contrat à distance à un consommateur de fournir à ce dernier « [son adresse géographique, ainsi que son numéro de téléphone], son numéro de télécopieur et son adresse électronique, lorsqu'ils sont disponibles, pour permettre au consommateur de le contacter rapidement et de communiquer avec lui efficacement ». Pour l'avocat général, « ce qui importe, ce n'est pas tant le moyen de communication considéré dans l'abstrait que la capacité concrète, c'est-à-dire envisagée par rapport aux spécificités du contexte dans lequel se déroule la transaction, d'assurer que le consommateur puisse contacter rapidement le professionnel et communiquer avec lui efficacement et que les informations soient fournies sous une forme claire et compréhensible »⁸². Il ne peut, à ce titre, être imposé au professionnel de communiquer, dans tous les cas, un numéro de téléphone au consommateur. D'autres moyens de communication doivent donc pouvoir être proposés, tels que par exemple une messagerie instantanée ou un système de rappel téléphonique⁸³.

De la même manière, en matière de services de paiement, si le prestataire doit prévoir, en plus de son adresse géographique et de son adresse électronique, un autre moyen permettant à l'utilisateur de rentrer en communication avec lui, ledit moyen ne sera pas nécessairement un numéro de téléphone. Une telle conclusion s'impose d'autant plus qu'en matière de services de paiement, à l'inverse des législations précitées relatives au commerce électronique et à la protection du consommateur, ni la DSP 2 ni sa loi belge de transposition ne contiennent d'exigence particulière de rapidité et d'efficacité du moyen de communication proposé.

⁸⁰ *Ibid.*, point 32. La Cour, toutefois, semble privilégier le numéro de téléphone comme moyen efficace et direct pour entrer en contact avec le prestataire, dans la mesure où elle estime préférable de proposer un accès à une voie de communication non électronique, ce que le numéro de téléphone constitue par excellence ; voy. à cet égard C.J., arrêt *deutsche internet versicherung*, 16 octobre 2008, C-298/07, points 36, 39 et 40. L'impact d'une telle jurisprudence, privilégiant *in fine* la communication du numéro de téléphone, nous semble devoir être relativisé. Tout d'abord, la Cour s'est prononcée en 2008, à une époque où internet, et en particulier l'internet mobile, n'était pas développé comme aujourd'hui, de sorte qu'il était envisageable de n'avoir, par moment, qu'un accès très limité à des moyens de communication électronique. Il n'est donc pas certain que la nuance qu'elle insère dans son arrêt soit aujourd'hui encore pertinente.

⁸¹ Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, J.O.U.E., L 304, 22 novembre 2011.

⁸² Conclusions de l'avocat général G. PITRUZZELLA, présentées le 28 février 2019, C.J., affaire *Bundesverband der Verbraucherzentralen und Verbraucherverbände, Verbraucherzentrale Bundesverband e. V. c. Amazon EU Sàrl*, C-649/17, EU:C:2019:165, point 54.

⁸³ *Ibid.*, point 118.

Par ailleurs, le prestataire doit communiquer « les coordonnées de l'autorité de contrôle prudentielle compétente et le registre [...] dans lequel [il] est inscrit en vue de son agrément, ainsi que son numéro d'enregistrement ou un moyen équivalent d'identification de ce registre »⁸⁴. À titre d'exemple, les établissements de paiement agréés en Belgique ont dû obtenir leur agrément auprès de la Banque nationale de Belgique, après la soumission d'un dossier spécifique d'agrément et leur enregistrement sur la liste des établissements de paiement agréés sur le territoire belge⁸⁵.

L'exigence d'information relative au prestataire paraît classique. Il semble évident en effet d'avoir à s'identifier pour pouvoir contracter. Une telle exigence est néanmoins essentielle dès lors qu'elle permet à l'utilisateur de s'assurer de l'identité et des habilitations de la personne avec qui il entend contracter pour bénéficier de services de paiement, services éminemment sensibles dès lors qu'ils touchent les fonds de l'utilisateur concerné, et leur protection. L'utilisateur sera ainsi rassuré⁸⁶ mais également responsabilisé : il peut vérifier lui-même que le prestataire qu'il sollicite est bien enregistré auprès de l'autorité prudentielle qu'il annonce⁸⁷. Côté prestataire, la première catégorie d'informations a également son importance : elle permet aux nouveaux entrants de montrer au grand public qu'ils sont titulaires de l'ensemble des autorisations nécessaires pour offrir un certain nombre de services et s'inscrire en tant que concurrents légitimes des grandes banques dont la renommée n'est plus à faire sur certains services de paiement.

26. Informations sur l'utilisation d'un service de paiement (art. VII.22, 2^o, du CDE). – L'article VII.22, 2^o, du CDE impose au prestataire de fournir un ensemble d'informations sur les services de paiement qu'il propose à l'utilisateur.

Le prestataire doit tout d'abord indiquer « une description des principales caractéristiques du service de paiement à fournir ». Il s'agit ici d'un pendant à l'obligation existant en matière de contrat à distance ne portant pas sur des services financiers, qui exige de fournir au moins les principales caractéristiques du bien ou du service proposé à la vente à distance⁸⁸. Sur ce point, le législateur belge s'est voulu plus précis que ne l'est la directive lorsqu'un

⁸⁴ Art. VII.22, 1^o, b), du CDE.

⁸⁵ Art. 9 et s. de la loi du 11 mars 2018 précitée.

⁸⁶ Pour rappel, renforcer la confiance des consommateurs à l'égard des marchés de paiement compte parmi les objectifs annoncés de la DSP 2 ; voy. en ce sens le considérant n^o 6 de la DSP 2.

⁸⁷ Conformément à l'article 8 de la loi du 11 mars 2018 précitée, la Banque nationale de Belgique « tient une liste des entités habilitées à fournir des services de paiement en Belgique », « publie la liste sur son site internet et actualise régulièrement les informations qu'elle contient ». Ainsi, toute personne souhaitant vérifier le statut et l'agrément d'un prestataire et s'assurer qu'il détient bien l'agrément qu'il annonce peut vérifier sur cette liste officielle et accessible à tous sur le site de la Banque nationale de Belgique s'il y est inscrit ou non. À titre d'exemple, le 23 avril 2019, le site de la Banque nationale de Belgique listait 24 établissements de paiement agréés en Belgique, voy. www.nbb.be/fr/supervision-financiere/controle-prudentiel/domaines-de-controle/etablisements-de-paiement-et-75.

⁸⁸ Voy. à cet égard, l'article VI.45, 1^o, du CDE.

instrument est intégré dans les services de paiement fournis. Ainsi, dans ce cas, le prestataire doit communiquer l'ensemble des utilisations possibles dudit instrument de paiement. La loi définit l'instrument de paiement comme « tout dispositif personnalisé et/ou ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement et auquel l'utilisateur de services de paiement a recours pour initier un ordre de paiement »⁸⁹. Le plus connu est l'instrument de paiement lié à une carte de crédit ou de débit, qui permet d'initier un virement via son espace *home-banking* ou de réaliser un paiement dans un point de vente. Le législateur⁹⁰ précise que pour la description des utilisations de l'instrument, on peut se référer aux dispositions légales applicables à l'instrument de transfert électronique de fonds⁹¹. Cette description devrait ainsi comporter notamment une description succincte de l'instrument et de son fonctionnement, les différentes opérations pouvant être effectuées par l'instrument ainsi qu'une description succincte des transactions, une indication des caractéristiques techniques minimales et en particulier des limitations techniques de l'instrument, une indication du territoire sur lequel l'instrument peut être utilisé, etc.⁹².

Le législateur tend ainsi à ajouter à une liste déjà bien précise un ensemble d'informations non prévues par la directive. On s'interroge dès lors sur la compatibilité de cet ajout, même implicite⁹³, opéré par le législateur, alors que la DSP 2 précise très clairement que les États ne peuvent pas adopter de dispositions en matière d'information qui soient différentes de celles qu'elle établit⁹⁴.

Le prestataire doit ensuite communiquer un certain nombre d'informations ayant trait notamment à la possibilité ou non de convenir de limites de dépenses, aux informations précises ou à l'identifiant unique que l'utilisateur doit fournir aux fins de l'initiation ou de l'exécution correcte de son ordre de paiement, etc. Les seules différences qui ont été intégrées avec la transposition de la DSP 2 sont l'insertion des informations relatives (1) aux nouveaux services d'initiation de paiement concernant le consentement de l'utilisateur et les informations ou l'identifiant à fournir pour permettre l'initiation du paiement, et (2) aux droits spécifiques de l'utilisateur d'un instrument lié à une carte cobadgée⁹⁵. Le cobadgeage, notion ajoutée par la DSP 2, renvoie à l'insertion du « logo d'un réseau partenaire sur une carte de paiement (CB,

⁸⁹ Art. 1.9, 10^e, du CDE.

⁹⁰ Projet de loi n° 3131/001 précité, p. 30, renvoyant au projet de loi n° 2179/001 précité, p. 40.

⁹¹ L'exposé des motifs se réfère précisément à la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, M.B., 17 août 2002, abrogée depuis lors par la loi précitée du 10 décembre 2009 relative aux services de paiement.

⁹² Projet de loi n° 2179/001 précité, pp. 40 et 41.

⁹³ Il ne s'opère qu'à la lecture de l'exposé des motifs de la loi du 10 décembre 2009, auquel l'exposé des motifs de la loi de transposition du 19 juillet 2018 renvoie expressément.

⁹⁴ Voy. l'article 107, § 1^{er} et le considérant n° 54 de la DSP 2.

⁹⁵ Le cobadgeage fait l'objet d'une des nouvelles définitions consacrées par la DSP 2. Il désigne, conformément à l'article 4, 48^e, « l'inclusion de deux ou de plusieurs marques de paiement ou applications de paiement de la même marque de paiement sur le même instrument de paiement ».

Visa, MasterCard...)⁹⁶. En France par exemple, la majorité des cartes portent le logo « CB »⁹⁷ et sont cobadgées avec un autre système de paiement, en général Visa ou MasterCard⁹⁸. Au regard du cobadgeage, l'utilisateur consommateur doit bénéficier d'une information claire de ses droits et des possibilités de choix qui y sont liées⁹⁹. Il doit, par exemple, être informé qu'il peut, dans certaines circonstances, demander que deux ou plusieurs marques soient apposées sur l'instrument de paiement lié à sa carte¹⁰⁰.

27. Les informations relatives aux frais, aux taux d'intérêt et aux taux de change (art. VII.22, 3^e, du CDE). – Le prestataire doit indiquer à l'utilisateur tous les frais qu'il devra lui payer, et le cas échéant, la ventilation de ceux-ci, en ce compris les frais payables liés aux modalités et à la fréquence selon lesquelles les informations prévues par la loi sont communiquées¹⁰¹. Il doit ensuite l'informer des taux d'intérêt et de change à appliquer le cas échéant.

28. Les informations relatives à la communication entre le prestataire et l'utilisateur (art. VII.22, 4^e, du CDE). – L'utilisateur doit être informé des moyens de communication qui seront utilisés aux fins de la transmission d'informations ou de notifications entre les parties, en ce compris les équipements et logiciels qui sont mis à disposition de l'utilisateur à ces fins. L'utilisateur doit également être informé des modalités et de la fréquence selon lesquelles les informations légalement prévues seront communiquées, ainsi que de la ou les langues dans lesquelles le contrat-cadre sera conclu et la communication effectuée en cours d'exécution dudit contrat. Le prestataire, enfin, doit rappeler à l'utilisateur son droit¹⁰² de demander, à tout moment pendant l'exécution du contrat-cadre, à recevoir les termes contractuels et les informations listées à l'article VII.22 sur un support durable¹⁰³.

⁹⁶ D. HELLEPEE, *L'univers de la monétique – Histoire, fonctionnement et perspectives*, Domptin, France, Carrefour du Net, 2009, p. 30.

⁹⁷ Le logo « CB » renvoie au logo du Groupement d'Intérêt Economique Cartes Bancaires ou « GIE CB ». Ce groupement a été créé en France en 1984 et regroupe près de 120 établissements prestataires de services de paiement (voy. le site internet du groupement <http://www.cartes-bancaires.com/fr>, consulté le 23 avril 2019). L'une des missions du GIE CB est d'assurer l'interbancaire au sein du système CB. Pour le GIE CB, le système CB est « l'écosystème qui permet à la carte CB d'être acceptée quelle que soit l'enseigne de la banque du commerçant et celle du client » (voy. la page « Fondamentaux / Interbancaire » du site internet du GIE CB <http://www.cartes-bancaires.com/fr/missions/fondamentaux>, consulté le 23 avril 2019).

⁹⁸ Voy. à cet égard la décision n° 13-D-17 de l'Autorité française de la concurrence du 20 septembre 2013 relative à des pratiques de MasterCard relevées dans le secteur des cartes de paiement, point 19.

⁹⁹ Voy. en ce sens, le projet de loi n° 3131/001 précité, p. 30.

¹⁰⁰ Art. 8, 2, du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, J.O.U.E., L 123, 19 mai 2015 ; sur les règles de transparence en matière de marques de paiement, voy. en particulier, A.-C. ROUAUD, « La nouvelle réglementation européenne relative aux systèmes de cartes de paiement et aux commissions interbancaires », *R.I.S.F.-I.J.F.S.*, 2015/4, p. 75.

¹⁰¹ Ce point provient de la transposition de la DSP 2.

¹⁰² Légalelement prévu par l'article VII.23 du CDE.

¹⁰³ Sur la notion de « support durable » de l'obligation d'information relative aux services de paiement, voy. *infra*, section 1, § 4, C.

29. Les informations relatives aux mesures de protection et aux mesures correctives à prendre par le prestataire et par l'utilisateur (art. VII.22, 5°, du CDE). – Le prestataire de services de paiement joue un rôle important en ce que, outre la conformité aux obligations de sécurité qui lui incombe¹⁰⁴, il doit fournir à l'utilisateur les informations nécessaires lui permettant de participer utilement à la prévention, et le cas échéant, à la correction d'opérations de paiement non autorisées, mal initiées ou mal exécutées¹⁰⁵. Le prestataire contribue ainsi, en lui délivrant une information correcte et suffisante, à la participation et à la responsabilisation de l'utilisateur pour assurer la sécurité de ses services et instruments de paiement¹⁰⁶.

À ce titre, le prestataire lui présente les mesures de prudence qu'il devra adopter pour préserver la sécurité de son instrument de paiement, ainsi que la ou les notifications qu'il devra soumettre lorsqu'il aura connaissance d'une perte, d'un vol, d'un détournement ou de toute utilisation de son instrument de paiement¹⁰⁷.

La DSP 2 ajoute que le prestataire doit en outre communiquer à l'utilisateur des informations sur la procédure sécurisée mise en œuvre pour la notification à laquelle il procédera, le cas échéant, en cas de soupçon de fraude, de fraude avérée ou de menaces pour la sécurité.

Par ailleurs, s'il décide d'user d'une telle faculté, le prestataire doit informer l'utilisateur des conditions dans lesquelles il se réserve le droit de bloquer l'instrument de paiement en question.

En cas d'opérations de paiement non autorisées, la loi¹⁰⁸ prévoit une répartition précise des obligations et responsabilités respectives entre le prestataire et l'utilisateur de services de paiement¹⁰⁹. Le prestataire doit fournir à l'utilisateur une explication précise sur cette répartition légale des responsabilités. La formulation de ces informations doit être particulièrement bien soignée et se conformer de manière stricte à la loi. En toute hypothèse, le prestataire ne pourra en aucun cas prévoir dans son contrat-cadre de clauses qui alourdiraient la responsabilité de l'utilisateur en cas d'opérations non autorisées. Les règles de partage de responsabilités prévues notamment à l'article VII.44 sont impératives (sous réserve qu'il n'y soit pas dérogé dans le cas de l'utilisateur non consommateur), de sorte que toute règle qui s'en éloignerait en alourdissant la responsabilité de l'utilisateur devrait être considérée comme nulle de plein droit¹¹⁰.

¹⁰⁴ Sur ce point, voy. *infra*, section 2, § 2, A.

¹⁰⁵ Sur ces deux notions, voy. *infra*, section 2, § 1, A.

¹⁰⁶ Il s'agira pour le prestataire, d'une certaine manière, d'expliquer à l'utilisateur quelles sont les obligations et responsabilités en termes de sécurité qui lui incombe légalement (ou, en d'autres termes, de les lui rappeler, lesdites obligations étant déjà inscrites dans la loi).

¹⁰⁷ Conformément à l'article VII.38, § 1^{er}, 2^o, du CDE ; sur ce point, voy. *infra*, section 2, § 3, A.

¹⁰⁸ Art. VII.43 et VII.44 du CDE.

¹⁰⁹ Sur cette répartition de responsabilités, voy. *infra*, section 2, § 3, C.

¹¹⁰ Voy. en ce sens le considérant n° 72 de la DSP 2 et article VII.2, § 4, du CDE qui dispose, précisément, que « toute stipulation contraire aux dispositions du présent livre et de ses arrêtés d'exécution est interdite et nulle de plein droit pour autant qu'elle vise à restreindre les droits des consommateurs ou à aggraver

Par ailleurs, le prestataire doit fournir un certain nombre d'informations concernant la responsabilité qu'il endosse pour l'initiation ou l'exécution correcte de l'opération de paiement¹¹¹.

Enfin, il doit indiquer à l'utilisateur les conditions de remboursement d'opérations de paiement initiées par ou via le bénéficiaire du paiement, qu'il appliquera, le cas échéant¹¹².

30. Les informations relatives à la modification et à la résiliation du contrat-cadre (art. VII.22, 6°, du CDE). – La loi permet au prestataire de services de paiement de proposer à l'utilisateur une modification du contrat-cadre. Ladite proposition de modification devra être communiquée selon des modalités identiques à celles imposées pour la communication de l'ensemble des informations obligatoires visées dans la présente partie¹¹³ (en d'autres termes, la proposition sera « fournie » sur un « support durable »¹¹⁴). La modification doit alors être proposée à l'utilisateur « au plus tard deux mois avant la date proposée [par le prestataire] pour son entrée en vigueur »¹¹⁵. La DSP 2 ajoute que l'utilisateur a la faculté d'accepter ou de rejeter ladite modification avant la date d'entrée en vigueur proposée¹¹⁶.

Le législateur laisse la possibilité au prestataire et à l'utilisateur de convenir contractuellement qu'en cas de modification du contrat-cadre proposée par le prestataire, l'utilisateur qui ne notifie pas son rejet de ladite modification avant la date d'entrée en vigueur proposée sera réputé avoir accepté cette modification¹¹⁷. On comprend qu'à l'inverse, l'utilisateur qui rejette la modification envisagée doit notifier ce rejet au prestataire avant son entrée en vigueur. S'il ne le fait pas, il sera réputé accepter la modification. La loi ne précise pas la forme que doit revêtir le rejet de la modification par l'utilisateur. Le mot « notification » nous indique néanmoins qu'un tel rejet doit être exprès et communiqué au prestataire.

À défaut de rejet exprès de la modification proposée, l'utilisateur sera réputé avoir accepté la modification. Une telle acceptation implicite est ainsi soumise à une double condition : (1) les parties doivent s'être accordées contractuellement sur ce point, et (2) le prestataire est tenu d'informer l'utilisateur qu'il est réputé accepter toute modification du contrat-cadre dès lors qu'il ne notifie pas son rejet avant l'entrée en vigueur prévue pour la modification.

leurs obligations » ; Bruxelles, 19 avril 2013, R.D.C., 2015, p. 185, note R. STEENNOT, cité dans J.-B. HUBIN et H. JACQUEMIN, « Chronique de jurisprudence (2012-2014) », R.D.T.L., 2015, n° 59-60, pp. 20 et 21.

¹¹¹ Art. VII.55/3 à VII.55/6 du CDE.

¹¹² Art. VII.46 et VII.47 du CDE.

¹¹³ Art. VII.24, § 1^{er}, du CDE, selon lequel la modification du contrat-cadre proposée par le prestataire de services de paiement doit être faite « selon les modalités prévues à l'article VII.21, § 1^{er} » du CDE.

¹¹⁴ Sur ces notions, voy. *infra*, section 1, § 4, C.

¹¹⁵ Art. VII.24, § 1^{er}, du CDE.

¹¹⁶ Art. 54, § 1^{er}, de la DSP 2 ; art. VII.24, § 1^{er}, du CDE.

¹¹⁷ Art. VII.24 du CDE.

Une modification du contrat-cadre proposée unilatéralement par le prestataire devient ainsi, par l'acceptation implicite de cette modification par l'utilisateur du fait de l'écoulement d'un laps de temps déterminé, une modification conventionnelle du contrat-cadre¹¹⁸. Pour Patrick Wéry, « la modification du contrat par les parties est [...] autorisée. Aux prises avec un événement dont elles n'avaient pas prévu la survenance, les parties ont toujours la possibilité de refaçonner, de commun accord, leur contrat [...] »¹¹⁹. Une telle modification sera parfois rendue nécessaire à la suite d'un changement de la loi ou d'un élément de fait (le changement du siège social du prestataire par exemple). Le législateur, en matière de services de paiement, ne fait en revanche aucune distinction selon que la modification du contrat-cadre a trait ou non à une obligation essentielle du contrat. Il précise néanmoins que la modification ne pourra porter sur « de nouveaux services [qui s'ajouteraient] au contrat-cadre initial, par exemple la mise à disposition d'une carte de paiement en combinaison avec le compte de paiement existant. Il s'agit alors d'un contrat complémentaire auquel les dispositions de ce titre, concernant l'information préalable etc., sont d'application. »¹²⁰

Interrogeons-nous un instant sur le caractère véritablement « conventionnel » de la modification proposée par le prestataire et acceptée implicitement par l'utilisateur. Tout d'abord, la modification est envisagée et proposée unilatéralement par le prestataire à l'utilisateur, qui n'aura d'autre choix que de l'accepter implicitement (ou à tout le moins de ne pas s'y opposer) ou de la rejeter expressément. Aucune possibilité de négociation ou de reformulation n'est effectivement envisagée dans le chef de l'utilisateur. Par ailleurs, le législateur crée un cadre qui privilégie l'acceptation de la modification proposée unilatéralement par le prestataire. En effet, dans le cadre ainsi mis en place, l'utilisateur ne devra faire aucun effort pour accepter la modification. En revanche, il devra s'y opposer expressément pour la rejeter. Le législateur semble postuler, de manière probablement un peu aveugle, que l'utilisateur sera suffisamment diligent pour, d'une part, lire, comprendre et accepter la clause du contrat-cadre selon laquelle son silence, pendant un laps de temps déterminé, vaudra acceptation de la modification proposée par le prestataire, d'autre part, que l'utilisateur prendra effectivement connaissance de la modification ainsi proposée et l'acceptera, en conscience, par son silence. Dans la pratique, ladite clause contractuelle prévoyant l'acceptation implicite de la modification sera fréquemment insérée, pour ne pas dire « noyée », dans un ensemble d'autres clauses contractuelles, toutes aussi complexes les unes que les autres, aux yeux de bon nombre des utilisateurs. Prévoir dans de telles circonstances

¹¹⁸ Pour la distinction entre ces deux modalités de modification d'un contrat (« modification unilatérale » et « modification conventionnelle »), voy. en particulier P. WÉRY, « Titre 1 – La suspension et la modification du contrat », in *Droit des obligations – Volume 1*, Bruxelles, Larcier, 2011, pp. 886 et s., points n° 954 et s.

¹¹⁹ P. WÉRY, *ibid.*, p. 887, point n° 954.

¹²⁰ Projet de loi n° 2179/001 précité, p. 45.

une acceptation d'une modification du contrat-cadre qui ne sera qu'implicite, du fait de l'écoulement d'un laps de temps, et qui n'exige aucun effort actif de la part des utilisateurs revient à leur « forcer » la main pour qu'ils l'acceptent. Nous comprenons ici que le législateur a souhaité assurer au prestataire que les modifications qu'il propose unilatéralement seront, dans la majorité des cas, acceptées par les utilisateurs pour éviter, on suppose, que l'exécution de contrats-cadres ne soit bloquée par l'absence de réaction, consciente ou non, des utilisateurs. Il reste que le législateur fait ici un choix : celui, de l'exécution des contrats-cadres au détriment, dans une certaine mesure, du principe de la liberté contractuelle.

Le prestataire doit par ailleurs informer l'utilisateur que dans l'hypothèse où il rejette la modification proposée, il dispose alors du droit de résilier le contrat-cadre, sans frais, et avec effet immédiat, jusqu'à la date d'entrée en vigueur proposée par le prestataire. Une hésitation subsiste alors quant au sort du contrat-cadre lorsqu'une telle modification a été rejetée expressément par l'utilisateur sans que celui-ci n'ait été jusqu'à résilier pour autant le contrat-cadre dans son ensemble. En effet, la résiliation du contrat est présentée comme un droit de l'utilisateur dans la loi, et non comme une conséquence automatique du rejet notifié de la modification. Le contrat-cadre dans son état antérieur à la modification subsiste-t-il pour tel utilisateur uniquement ? Une réponse positive impliquerait pour les prestataires de services de paiement de maintenir en vigueur une version à l'égard de tel utilisateur, et une autre version à l'égard des autres. Un tel scénario nous semble, d'un point de vue pratique, difficilement envisageable.

Le législateur distingue en outre les modifications des taux d'intérêts ou de change des autres modifications du contrat-cadre envisagées précédemment. Ainsi, de telles modifications pourront s'appliquer immédiatement et sans préavis, sous réserve notamment de le prévoir dans le contrat-cadre¹²¹. Le législateur précise qu'il « peut être dérogé, à certaines conditions, à l'obligation d'information préalable de deux mois ou, le cas échéant, à toute forme de notification »¹²². Une obligation d'information particulière incombe alors au prestataire, qui doit informer l'utilisateur de toute modification des taux d'intérêt ou de change le plus rapidement possible, sauf dans l'hypothèse où les parties seront convenues d'une fréquence ou de modalités particulières de communication desdites informations¹²³. Le prestataire a en toute hypothèse la faculté d'appliquer sans préavis les taux d'intérêt ou de change qui seraient plus favorables à l'utilisateur¹²⁴.

Enfin, le prestataire doit communiquer à l'utilisateur les informations relatives à la durée du contrat, l'informer de son droit de résilier le contrat-cadre et

¹²¹ Art. VII.24, § 2, alinéa 1^{er}, du CDE.

¹²² Projet de loi n° 2179/001 précité, p. 46.

¹²³ Art. VII.24, § 2, alinéa 2, du CDE.

¹²⁴ Art. VII.24, § 2, alinéa 2, du CDE.

lui rappeler tout accord qui serait lié à cette résiliation, conformément aux articles VII.24, § 1^{er} et VII.25 du CDE¹²⁵.

31. Les informations relatives aux recours en cas de litige (art. VII.22, 7^o, du CDE). – Enfin, le prestataire a l'obligation de fournir à l'utilisateur toute information concernant le droit applicable au contrat-cadre et la juridiction compétente en cas de litige.

Il doit par ailleurs préciser à l'utilisateur que la loi¹²⁶ prévoit un ensemble de voies possibles de réclamation et de règlements extrajudiciaires des litiges. L'entité qualifiée instituée¹²⁷ pour « garantir et favoriser des procédures adéquates et efficaces de réclamation et de recours extrajudiciaires en vue du règlement des litiges qui opposent les bénéficiaires^[128] et leurs prestataires de services de paiement »¹²⁹ est l'ASBL Services de médiation des services financiers/*Ombudsdienst voor financiële diensten*, connue sous son abréviation Ombudsfm¹³⁰. Les prestataires de services de paiement sont tenus¹³¹ d'adhérer au règlement extrajudiciaire des litiges ainsi institué¹³².

Le prestataire de services de paiement a, à l'égard des réclamations éventuelles et des procédures de règlement extrajudiciaire des litiges, une obligation d'information particulière. Il doit indiquer l'adresse physique de l'instance à laquelle l'utilisateur pourra adresser ses réclamations, à savoir les coordonnées de ses propres services internes de réclamations, s'ils existent, celle de l'Ombudsfm, et, en toute hypothèse, celles de la Direction générale Inspection économique auprès du Service public fédéral Économie¹³³. Une telle obligation d'information est précisée par l'article XVI.4 du CDE relatif au règlement extrajudiciaire des litiges. Selon cet article, lorsque le prestataire est tenu « par

¹²⁵ Art. VII.22, 6^o, b) et c), du CDE.

¹²⁶ En l'occurrence le livre XVI du CDE.

¹²⁷ Conformément aux conditions prévues à l'article XVI.25 du CDE.

¹²⁸ L'article VII.216 du CDE prévoyant l'institution du règlement extrajudiciaire des plaintes en matière de services financiers limite le champ des litiges concernés aux « litiges entre d'une part, un prestataire de services de paiement [...] et, d'autre part, un consommateur ». Les litiges qui surviendraient entre un prestataire de services de paiement et un utilisateur non consommateur ne sont pas couverts par la procédure de règlement extrajudiciaire des litiges. L'acte de constitution de l'ASBL Ombudsfm, l'entité qualifiée instituée en matière financière, ne vise également que les litiges avec les consommateurs, voy. l'article 5 de l'acte de constitution d'Ombudsfm, www.ombudsfm.be/sites/default/files/15102252.pdf.

¹²⁹ Art. XVI.63/3, § 1^{er}, du CDE.

¹³⁰ Art. VII.63/3 et VII.216 du CDE.

¹³¹ Il doit être noté que dans d'autres domaines, le recours et l'adhésion à une entité de médiation qualifiée, conformément au livre XVI du CDE, ne seront pas nécessairement une obligation légale. Une telle adhésion pourra être le résultat d'un engagement volontaire de la part de l'entreprise de reconnaître la compétence de telle entité qualifiée de médiation. Par exemple, l'ombudsman du commerce, reconnu depuis le 4 avril 2017 comme entité qualifiée de règlement extrajudiciaire des litiges de consommation, conformément au titre 4 du livre XVI du CDE, n'est compétent que pour connaître des litiges de consommation soulevés à l'encontre des entreprises qui se seront préalablement, volontairement, enregistrées auprès de lui. Mais un tel enregistrement n'est pas obligatoire en vertu de la loi. À l'inverse, les prestataires de services de paiement sont tenus, légalement, d'adhérer à l'Ombudsfm.

¹³² Art. VII.63/3, § 4, du CDE.

¹³³ Art. VII.22, 7^o, du CDE.

la loi [...] à recourir à une procédure de règlement extrajudiciaire des litiges de consommation, elle en informe le consommateur de manière claire, compréhensible et aisément accessible »¹³⁴. Il est ajouté que les informations ainsi communiquées doivent permettre « d'accéder à des informations détaillées sur les caractéristiques et les conditions d'utilisation de ces moyens de règlement extrajudiciaire des litiges de consommation et comprennent les coordonnées et l'adresse du site internet de l'entité ou des entités qualifiées concernées »¹³⁵. Il est enfin précisé que lesdites informations doivent être, le cas échéant, « disponibles sur le site internet ainsi que dans les conditions générales de vente de l'entreprise »¹³⁶. Le prestataire devra s'attacher tout particulièrement à communiquer de manière suffisante, tant dans ses conditions contractuelles que sur son site, les informations permettant à l'utilisateur d'être au courant des modes alternatifs à la procédure judiciaire de règlement des litiges dont il peut bénéficier et de la manière dont il peut les actionner, le cas échéant.

Enfin, une obligation d'information supplémentaire incombe aux prestataires lorsqu'ils proposent la conclusion de contrats-cadre en ligne, qui constitueraient des contrats de service au sens du règlement européen relatif au règlement en ligne des litiges de consommation¹³⁷. Le contrat de service concerné est le contrat « par lequel le professionnel ou son intermédiaire propose, sur un site internet ou par d'autres moyens électroniques, des biens ou des services que le consommateur commande sur le même site internet ou par d'autres moyens électroniques »¹³⁸. Il s'agira, par exemple, du contrat conclu en ligne portant sur l'ouverture d'un compte à vue ou d'un compte épargne. Ce règlement relatif au RLLC a mis en place une plateforme (dite « plateforme RLL », pour règlement en ligne des litiges, ou « plateforme ODR » pour son équivalent anglais *online dispute resolution*) devant constituer « un guichet unique pour les consommateurs et les professionnels souhaitant régler par la voie extrajudiciaire un litige »¹³⁹. La plateforme ne peut connaître que des « litiges concernant des obligations contractuelles découlant de contrats de vente ou de service en ligne entre un consommateur résidant dans l'Union et un professionnel établi dans l'Union »¹⁴⁰. Dans une telle hypothèse, le prestataire devra inclure sur son site internet un lien vers la plateforme RLL¹⁴¹. Il devra, de plus, informer « les consommateurs de l'existence de la plateforme de RLL et de la possibilité d'y recourir pour régler leurs litiges »¹⁴². Le

¹³⁴ Art. XVI.4, § 1^{er}, du CDE.

¹³⁵ Art. XVI.4, § 2, alinéa 1^{er}, du CDE.

¹³⁶ Art. XVI.4, § 2, alinéa 2, du CDE.

¹³⁷ Règlement (UE) n° 524/2013 du Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 2009/22/CE (règlement relatif au RLLC), *J.O.U.E.*, L 165, 18 juin 2013.

¹³⁸ Art. 4, d) et e), du règlement relatif au RLLC.

¹³⁹ Art. 5, § 2, du règlement relatif au RLLC.

¹⁴⁰ Art. 2 du règlement relatif au RLLC.

¹⁴¹ Art. 14, § 1^{er} et § 2, du règlement relatif au RLLC.

¹⁴² Art. 14, § 2, du règlement relatif au RLLC.

règlement ajoute que « ces informations sont aussi fournies, le cas échéant, dans les conditions générales applicables aux contrats de vente et de service en ligne »¹⁴³.

32. Conclusion concernant les informations générales à fournir en cas de contrat-cadre. – L'ensemble de ces informations se retrouvera, dans la plupart des cas, au sein du contrat-cadre relatif au service de paiement envisagé, ou pour employer une notion plus usitée en pratique, au sein des conditions bancaires générales ou du règlement général des opérations. Ces informations prendront par conséquent la forme de clauses dites contractuelles. Pour autant, l'on peut s'interroger, à l'égard de certaines de ces clauses, sur ce qu'il en reste de contractuel. Leur but, en effet, est essentiellement d'expliquer et/ou de rappeler à l'utilisateur le contenu de la loi, et en vertu de cette loi, ses droits et responsabilités. On pense, en particulier à la clause qui rappellera le partage de responsabilité entre le prestataire et l'utilisateur payeur en cas d'opération non autorisée. Sur ce point, lorsqu'il conclut avec un utilisateur consommateur, le prestataire est non seulement tenu de lui fournir un certain nombre d'informations minimales, mais en outre, il n'a que très peu de marge de manœuvre concernant le contenu même de ces informations.

La liberté contractuelle étant réduite, à l'égard de certaines de ces clauses, à peau de chagrin, ne serait-il pas souhaitable pour le législateur d'aller jusqu'au bout du processus, en proposant des clauses contractuelles types ou standardisées que le prestataire aurait la liberté de reprendre ou non¹⁴⁴? Une telle démarche aurait l'avantage de permettre au prestataire qui les reprend de s'assurer de fournir des informations suffisantes et conformes au prescrit légal et d'éviter ainsi les éventuels dérapages pouvant mener parfois à des contentieux inutilement coûteux pour les utilisateurs concernés. Il n'est toutefois pas certain que le législateur belge puisse prendre une telle liberté au regard de la DSP 2¹⁴⁵.

¹⁴³ Art. 14, § 2, du règlement relatif au RLLC.

¹⁴⁴ Le législateur belge et le législateur européen de la directive 2011/83 relative aux droits des consommateurs ont fait ce choix pour la fourniture des informations légales obligatoires concernant le droit de rétractation en matière de contrat à distance ne portant pas sur des services financiers. Ainsi, le paragraphe 3 de l'article VI.45 prévoit que « les informations visées au paragraphe 1^{er}, 8^o, 9^o et 10^o, peuvent être fournies au moyen des informations standardisées sur la rétractation figurant sur le modèle visé à [l'annexe 1] du présent livre. L'entreprise a respecté les obligations d'information énoncées aux points précités du paragraphe 1^{er}, 8^o, 9^o et 10^o, si elle a fourni lesdites informations au consommateur, correctement complétées ». Hervé Jacquemin précise qu'un choix similaire a également été opéré dans le cadre de la loi sur les crédits à la consommation (voy. les articles VII.70 et VII.71 du CDE renvoyant aux formulaires « informations européennes normalisées en matière de crédit aux consommateurs (SECCI) figurant aux annexes 1 et 2 du livre VII du CDE) et de celle sur le *time-sharing* (voy. les annexes de la loi du 28 août 2011 relative à la protection des consommateurs en matière de contrats d'utilisation de biens à temps partagé, de produits de vacances à long terme, de revente et d'échange, M.B., 16 septembre 2011). Il s'annonce enthousiaste à l'égard d'une telle démarche, tout en la nuanciant, néanmoins, dès lors que, selon lui, « des efforts devront encore être faits pour s'assurer que les informations ainsi transmises sont effectivement lues et comprises par les consommateurs », voy. H. JACQUEMIN, « Heurs et malheurs du formalisme contractuel comme mécanisme de protection du consommateur », *op. cit.*, pp. 277-278.

¹⁴⁵ Voy. l'article 107, § 1^{er} et le considérant n° 54 de la DSP2.

b) *Les informations ponctuelles relatives à l'opération individuelle réalisée en vertu du contrat-cadre*

33. Les informations préalables à l'opération de paiement individuelle. – De manière générale, à la demande de l'utilisateur payeur, et préalablement à toute transaction de paiement individuelle relevant d'un contrat-cadre, le prestataire communique des informations explicites sur le délai d'exécution maximal de ladite opération, sur les frais qui doivent être payés par le payeur et sur, le cas échéant, la ventilation de ces frais¹⁴⁶. Le législateur précise qu'un « chiffre global relatif à tous les frais est insuffisant lorsque le contrat-cadre prévoit une ventilation des éléments de frais » et que l'utilisateur « doit pouvoir vérifier à première vue la validité de tous les frais demandés »¹⁴⁷.

34. Les informations à communiquer après l'opération de paiement individuelle. – Le prestataire doit par ailleurs communiquer, en toute hypothèse, et sans que cela ne lui soit demandé par l'utilisateur, des informations relatives à l'opération de paiement qui a eu lieu¹⁴⁸. Pour le législateur, il s'agit là de « rendre les opérations de paiement transparentes et donner au payeur une « vue » claire sur tous les frais liés à l'opération »¹⁴⁹. Cela pourra prendre la forme d'extraits de comptes, envoyés par voie postale ou imprimés par des automates bancaires, ou d'extraits stockés dans l'espace personnel de l'utilisateur sur le site internet de son prestataire.

Ainsi, après que le montant d'une opération de paiement individuelle a été débité sur le compte de l'utilisateur, ou dans l'hypothèse où l'utilisateur ne disposerait pas de compte, après réception par le prestataire de l'ordre de paiement, l'utilisateur payeur doit recevoir un ensemble d'informations sur l'opération qui vient d'être exécutée, et ce sans tarder, ou lorsque le contrat-cadre le prévoit, périodiquement, et en toute hypothèse au minimum une fois par mois¹⁵⁰. L'enjeu est ici de permettre à l'utilisateur de vérifier rapidement les différents mouvements de son compte bancaire ou de sa carte de crédit pour être en mesure de procéder au plus vite, le cas échéant, à la notification auprès de son prestataire de toute opération qui lui paraîtrait litigieuse¹⁵¹.

Dans cette optique, le prestataire de services de paiement communiquera à l'utilisateur payeur les informations lui permettant d'identifier l'opération de paiement en question, son montant exprimé dans la devise utilisée, le montant des frais appliqués et, le cas échéant, la ventilation de ces montants ou l'intérêt dû par le payeur, le taux de change éventuellement applicable et le

¹⁴⁶ Art. VII.26 du CDE.

¹⁴⁷ Projet de loi n° 3131/001 précité, p. 33.

¹⁴⁸ Lesdites informations à communiquer sont alors similaires à celles que le prestataire doit communiquer en cas d'opération de paiement isolée qui ne serait pas couverte par un contrat-cadre ; voy., à cet égard, *supra*, section 1, § 3, A, 1.

¹⁴⁹ Projet de loi n° 2179/001 précité, p. 50.

¹⁵⁰ Art. VII.27 du CDE.

¹⁵¹ Sur une telle notification, voy. *infra*, section 2, § 3, A.

montant de l'opération de paiement après la conversion monétaire, ainsi que la date de valeur du débit ou la date de réception de l'ordre de paiement¹⁵². Le bénéficiaire de l'opération de paiement reçoit de son prestataire de services de paiement le même type d'informations¹⁵³.

3. Les informations à communiquer dans certains cas particuliers impliquant une conversion monétaire ou des frais spécifiques

35. Présentation des cas particuliers impliquant la communication d'informations supplémentaires. – Outre les informations précédemment mentionnées, l'utilisateur doit recevoir un certain nombre d'informations supplémentaires (1) dans l'hypothèse où l'opération de paiement implique une conversion monétaire ou (2) dans l'hypothèse où le bénéficiaire, le prestataire de services de paiement ou un tiers demande des frais ou offre une réduction aux fins de l'utilisation d'un instrument de paiement donné. De telles informations devront être communiquées, que l'opération envisagée soit une opération de paiement isolée ou une ou plusieurs opération(s) individuelle(s) couverte(s) par un contrat-cadre.

36. L'opération de paiement impliquant une conversation monétaire. – La première hypothèse concerne le cas où l'opération de paiement implique une conversion monétaire dans une devise spécifique. La loi veut que les paiements soient effectués dans la devise convenue entre les parties¹⁵⁴. Le législateur indique que, conformément à ce principe, « le payeur peut par exemple remettre de l'argent au "Money remitter" dans toute unité monétaire que ce dernier veut bien accepter »¹⁵⁵. Le prestataire doit, de manière générale, communiquer à l'utilisateur les informations utiles concernant le taux de change applicable à l'opération de paiement isolée¹⁵⁶ ou applicable aux opérations individuelles couvertes par un contrat-cadre¹⁵⁷.

Le législateur envisage toutefois trois cas particuliers dans lesquels le service de conversion monétaire dans une devise donnée est proposé par un tiers indépendant du prestataire de services de paiement de l'utilisateur payeur. La conversion monétaire peut être proposée : (1) au distributeur automatique de billets, (2) au point de vente, ou (3) par le bénéficiaire¹⁵⁸. Il peut, par exemple, s'agir du commerçant dans son magasin ou dans un restaurant¹⁵⁹. La DSP 2 a étendu cette hypothèse également aux distributeurs automatiques de billets¹⁶⁰.

¹⁵² Art. VII.27, § 1^{er}, du CDE.

¹⁵³ Art. VII.28, § 1^{er}, du CDE.

¹⁵⁴ Art. VII.10 du CDE.

¹⁵⁵ Projet de loi n° 3131/001 précité, p. 23.

¹⁵⁶ Art. VII.14 et VII.15, § 1^{er}, 3^o et 4^o, du CDE.

¹⁵⁷ Art. VII.22, 3^o, et VII.27, § 1^{er}, 3^o et 4^o, du CDE.

¹⁵⁸ Art. VII.10, § 2, du CDE.

¹⁵⁹ Projet de loi n° 3131/001 précité, p. 23.

¹⁶⁰ Art. 59, § 2, de la DSP 2 ; voy. le considérant n° 18 de la DSP 2 qui précise que : « Dans les situations transfrontalières, [l'exclusion des fournisseurs de distributeurs automatiques de billets du champ d'application de la DSP 2] pourrait se traduire par un double prélèvement pour un même retrait par le prestataire de

Ainsi, désormais, le fournisseur indépendant de distributeurs automatiques de billets proposant un service de conversion monétaire préalable à une opération de paiement sera également tenu à une obligation d'information particulière concernant la conversion monétaire envisagée¹⁶¹.

La partie qui propose ainsi à l'utilisateur un service de conversion monétaire est tenue de l'informer de tous les frais appliqués, ainsi que du taux de change qui sera utilisé aux fins de la conversion monétaire envisagée¹⁶². Le payeur doit, *in fine*, rester libre d'accepter ou de refuser le service de conversion monétaire proposé¹⁶³.

37. La partie demandant des frais ou proposant une réduction pour l'utilisation d'un instrument de paiement donné. – Par ailleurs, lorsque le bénéficiaire d'une opération de paiement demande des frais, ou offre une réduction, pour l'utilisation de tel ou tel instrument de paiement donné aux fins de l'opération envisagée, il devra en informer l'utilisateur avant l'initiation de l'opération¹⁶⁴. La même obligation d'information incombera au prestataire de services de paiement, ou à toute autre partie intervenant dans l'opération qui demandera des frais liés à l'utilisation d'un instrument donné¹⁶⁵. Le législateur avertit que ces dispositions doivent être lues « en même temps que les dispositions qui encadrent davantage le droit de demander ou non un supplément tel que visé à l'article 62 de la directive »¹⁶⁶. L'article 62 de la DSP 2 interdit notamment d'appliquer des frais dépassant les coûts directs supportés par le bénéficiaire pour l'utilisation de tel instrument de paiement donné, ou d'appliquer des frais au titre de l'utilisation d'instruments de paiement pour lesquels les commissions d'interchange sont réglementées¹⁶⁷.

La DSP 2 a procédé à une modification notable en vue de sanctionner le respect de ces obligations : désormais, l'utilisateur payeur ne sera tenu, le cas échéant, de s'acquitter des frais mentionnés dans le paragraphe précédent que s'il a été informé de leur montant avant l'initiation de l'opération de paiement¹⁶⁸.

services de paiement gestionnaire du compte et par le fournisseur de distributeurs automatiques de billets. Par conséquent, afin de maintenir la prestation de services de retrait d'espèces offerts aux distributeurs automatiques tout en garantissant la clarté quant aux frais de retrait, il convient de conserver l'exclusion [des fournisseurs de distributeurs automatiques de billets du champ d'application de la DSP 2] mais d'exiger des opérateurs de distributeurs automatiques qu'ils se conforment à certaines exigences de transparence de la présente directive ».

¹⁶¹ Projet de loi n° 3131/001 précité, p. 24.

¹⁶² Art. VII.10, § 2, alinéa 1^{er}, du CDE.

¹⁶³ Art. VII.10, § 2, alinéa 2, du CDE.

¹⁶⁴ Art. VII.11, alinéa 1^{er}, du CDE.

¹⁶⁵ Art. VII.11, alinéa 2, du CDE.

¹⁶⁶ Projet de loi n° 3131/001 précité, p. 24.

¹⁶⁷ Les commissions d'interchange sont réglementées par le chapitre II du règlement (UE) 2015/751 précité ; la commission d'interchange désigne, en vertu de l'article 2, 10), du règlement 2015/751, la « commission payée directement ou indirectement (à savoir par un tiers) pour chaque opération effectuée entre l'émetteur et l'acquéreur qui sont parties à une opération de paiement liée à une carte. La compensation nette ou les autres rémunérations convenues sont considérées comme faisant partie de la commission d'interchange ».

¹⁶⁸ Art. 62, § 3, de la DSP 2 ; art. VII.11, alinéa 3, du CDE.

B. Un contenu variable selon les caractéristiques du service de paiement

38. Différentes caractéristiques du service de paiement à prendre en compte. – Le contenu de l'obligation à communiquer variera selon que le contrat relatif au service de paiement sera conclu ou non à distance, selon que l'instrument de paiement ne permet que des opérations d'un montant faible, selon que le contrat envisagé est un contrat de crédit, ou encore selon que le contrat envisagé concerne un compte de paiement.

39. Le contrat conclu à distance. – Lorsque le contrat relatif à un service de paiement est conclu à distance, on devra tenir compte, pour déterminer le contenu de l'information devant être communiquée à l'utilisateur, en plus du livre VII du CDE, de certaines dispositions du livre VI, et en particulier de celles relatives aux contrats à distance portant sur des services financiers¹⁶⁹. Les services financiers sont définis comme « tout service ayant trait à la banque, au crédit, à l'assurance, aux retraites individuelles, aux investissements et aux paiements »¹⁷⁰. Les services de paiement sont donc englobés dans la notion de services financiers.

Ainsi, en cas de contrat-cadre conclu à distance, certaines informations que le livre VII rend obligatoires remplaceront des informations imposées par le livre VI. Les informations imposées par le livre VI non couvertes par le livre VII devront en revanche toujours être communiquées¹⁷¹.

40. L'instrument de paiement concernant exclusivement des opérations de faible montant. – L'obligation d'information sera allégée dans le cas d'instruments de paiement qui, conformément au contrat-cadre qui les couvre, ne concernent que des opérations de paiement n'excédant pas 30 euros ou, soit ont une limite de dépense de 150 euros, soit stockent des fonds dont le montant n'excède à aucun moment 150 euros¹⁷². Il est laissé la faculté au Roi de réduire ou de doubler les montants ici visés, voire, pour

les instruments prépayés, d'augmenter le plafond jusqu'à 500 euros. Une telle faculté n'a, à ce jour, pas été utilisée.

41. Les informations supplémentaires à communiquer en cas de contrat-cadre concernant l'ouverture d'un compte de paiement autorisant un dépassement et octroyant un crédit (art. VII.4 et VII.21, § 3, alinéa 2, du CDE). – Dans le cas du contrat-cadre concernant un compte de paiement autorisant un dépassement, le prestataire devra communiquer à l'utilisateur les informations relatives au taux débiteur¹⁷³ ainsi que, pour tout contrat de crédit, toute autre information que la loi exige en cas de contrat de crédit¹⁷⁴.

42. Les informations supplémentaires particulières à communiquer en cas de contrat-cadre relatif à un compte de paiement (art. VII.4/1 à VII.4/4 du CDE). – Lorsque le contrat-cadre est relatif à un compte de paiement, devront également être ajoutées à l'ensemble des informations mentionnées dans les paragraphes précédents des informations concernant (1) les frais liés aux comptes de paiement, (2) le changement de compte de paiement, et (3) l'accès à un compte de paiement assorti de prestations de base. Il est à noter que seul le consommateur bénéficie d'une telle obligation d'information. Cette obligation particulière d'information n'est pas issue de la transposition de la DSP 2, mais de la transposition d'une autre directive : la directive 2014/92/UE du 23 juillet 2014¹⁷⁵. L'objectif de cette directive est d'améliorer la transparence et la comparabilité des services et des frais associés aux comptes de paiement, en vue notamment de faciliter pour les consommateurs le changement de comptes de paiement et la comparaison entre les différentes offres existantes¹⁷⁶. Dans ce but, il a été opté pour « l'emploi d'une terminologie normalisée, associée à des informations ciblées sur les frais présentées sous une forme cohérente, et couvrant les services les plus représentatifs liés à un compte de paiement »¹⁷⁷. Un document dit d'information tarifaire, un glossaire, ainsi qu'un relevé de frais, dont les contenus et présentations sont déterminés au niveau de la directive¹⁷⁸, doivent ainsi être communiqués à l'utilisateur.

¹⁶⁹ Les dispositions en question sont les articles VI.54 à VI.63 du CDE, contenus dans la section 2 du chapitre 2 du livre VII du CDE ; l'obligation d'information imposée en cas de contrats portant sur des services financiers conclus à distance est issue de la directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, J.O.C.E., L 271, 2 octobre 2002.

¹⁷⁰ Art. I.8 du CDE.

¹⁷¹ L'article VII.6 prévoit que : « Lorsqu'un contrat relatif aux services de paiement est conclu à distance, les informations visées aux articles VII.14, VII.15, VII.21 et VII.22 remplacent les informations visées à l'article VI.55, § 1^{er}, du Code de droit économique, à l'exception du 2^o, c) à g), 3^o, a), d) et e), et 4^o, b). » ; les informations de l'article VI.55, § 1^{er}, qui devront toutefois être fournies sont relatives au service financier envisagé (par exemple : devra être fournie l'indication que le service financier est lié à des instruments qui impliquent des risques particuliers, du fait de leurs spécificités, ou des opérations à exécuter), au contrat à distance (par exemple : certaines informations relatives à l'existence ou l'absence du droit de rétractation) ou encore au recours potentiel (par exemple : l'existence d'un fonds de garantie ou d'autres mécanismes d'indemnisation). On notera ici que les informations à communiquer au titre de l'article VI.55 ne sont impératives qu'à l'égard du consommateur. Une telle obligation ne sera pas applicable en cas de contrat conclu avec un non-consommateur, pas même de manière supplétive.

¹⁷² Art. VII.9 du CDE.

¹⁷³ Listées à l'article VII.71, § 2, alinéa 2, du CDE.

¹⁷⁴ L'article VII.4 du CDE précise en effet que « les dispositions du [titre 3 relatif aux services de paiement] ne portent pas atteinte à d'autres dispositions légales contenues au sein du titre 4 du présent livre desquelles découleraient des exigences supplémentaires relatives à l'information préalable ou à des conditions, droits et obligations spécifiques en matière d'octroi de crédit aux consommateurs ».

¹⁷⁵ Directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base, J.O.U.E., L 257, 28 août 2014 ; cette directive a été transposée en droit belge par la loi du 22 décembre 2017 portant modification et insertion de dispositions en matière de comptes de paiement et de services de paiement dans différents livres du CDE (M.B., 12 janvier 2018).

¹⁷⁶ Voy. le considérant n° 9 de la directive 2014/92 précitée ; projet de loi portant modification et insertion de dispositions en matière de comptes de paiement et de services de paiement dans différents livres du CDE, résumé, Doc., Ch., 2017-2018, n° 2772/001, p. 3.

¹⁷⁷ Considérant n° 15 de la directive 2014/92 précitée.

¹⁷⁸ Art. 4 et 5 de la directive 2014/92 précitée ; art. VII.4/1 et VII.4/2 du CDE.

§ 4. La communication des informations

A. La charge de la preuve de la communication des informations

43. La charge de la preuve incombant au prestataire. – La charge de la preuve de l'accomplissement de l'obligation d'information ci-dessus développée, conformément aux modalités décrites dans le présent paragraphe, incombe au prestataire de services de paiement¹⁷⁹, à l'exception des informations sur les frais et conversions monétaires devant le cas échéant être délivrées par des tiers¹⁸⁰.

B. Le principe de gratuité de la communication des informations

44. Le principe de gratuité. – La communication des informations mentionnées aux paragraphes précédents doit être gratuite, en d'autres termes, sans frais pour l'utilisateur¹⁸¹.

Pour le législateur européen, d'une part, il doit être consacré un « droit des consommateurs à recevoir gratuitement les informations pertinentes avant d'être liés par un quelconque contrat de services de paiement », et d'autre part, « les consommateurs devraient être en mesure de réclamer des informations préalables et le contrat-cadre sur papier, sans frais, à tout moment au cours de la relation contractuelle, afin de pouvoir comparer les services et les conditions proposés par les prestataires de services de paiement et, en cas de litige, de vérifier leurs droits et obligations contractuels »¹⁸². Le législateur belge qualifie les informations développées dans les paragraphes précédents d'« informations de base prévues par la loi » et il précise qu'à leur égard, la « gratuité est absolue »¹⁸³.

Le principe de gratuité s'étend à l'information devant être communiquée tout au long de la durée d'exécution du contrat-cadre¹⁸⁴.

La mise à disposition du relevé des frais à laquelle le prestataire doit procéder, au regard des frais associés au compte de paiement, doit également être gratuite¹⁸⁵.

¹⁷⁹ Art. VII.8 du CDE.

¹⁸⁰ Voy. sur ce point *supra*, section 1, § 3, A, 1.

¹⁸¹ Art. VII.7 du CDE.

¹⁸² Considérant n° 59 de la DSP 2.

¹⁸³ Projet de loi n° 3131/001 précité, p. 22.

¹⁸⁴ L'article VII.7, § 1^{er}, du CDE applique le principe de gratuité à toutes « les informations fournies en vertu du [chapitre 2 du livre VII] ». L'article VII.23 du CDE prévoit le droit pour l'utilisateur de recevoir, sur demande, à tout moment, les termes contractuels du contrat-cadre et les informations visés à l'article VII.22 (à savoir l'ensemble des informations relatives au contrat développées *supra*, section 1, § 3, A, 2, a). Par ailleurs, la gratuité s'applique également pour la communication de l'ensemble des informations après l'exécution d'une opération de paiement individuelle prévue à l'article VII.27 du CDE (voy. sur ce point *supra*, section 1, § 3, A, 2, b). Le paragraphe 2 de cet article indique expressément que lorsque l'utilisateur payeur demande que lesdites informations soient communiquées périodiquement, une telle communication doit être gratuite également.

¹⁸⁵ Art. VII.4/2 du CDE.

45. Des frais exceptionnels. – Une exception, toutefois, est légalement prévue. Des frais pourront devoir être payés par l'utilisateur, dans certains cas, pour obtenir des informations, mais à des conditions strictes¹⁸⁶.

D'une part, de tels frais ne pourront être imputés à l'utilisateur que dans le cas où celui-ci demande davantage d'informations ou demande une communication des informations de base plus fréquente, ou par des moyens autres que ceux qui sont prévus par le contrat-cadre. D'autre part, ces frais devront être convenus contractuellement entre le prestataire et l'utilisateur. Enfin, de tels frais devront, en toute hypothèse, être raisonnables et conformes au coût réel supporté par le prestataire de services de paiement. Le législateur belge ajoute que « ces frais doivent être conformes aux frais réels de ce service administratif. Les frais non conformes, décourageant la demande d'informations de l'utilisateur, engendrant des recettes illégitimes ou encore pouvant être considérés comme un dédommagement ou une amende sont abusifs »¹⁸⁷.

C. Les modalités de la communication des informations

46. La forme et la langue des informations à communiquer. – Les informations devront être communiquées « dans des termes aisément compréhensibles et sous une forme claire et intelligible »¹⁸⁸. Elles devront être communiquées dans la ou les langues de la région linguistique dans laquelle le service de paiement est offert¹⁸⁹. À ce titre, pour le prestataire de services de paiement visant le marché belge dans son entièreté, les trois langues (néerlandais, français et allemand) devront être envisagées. Le législateur se montre toutefois assez souple, en laissant la possibilité, par dérogation, de convenir contractuellement avec l'utilisateur de la langue de l'information¹⁹⁰.

47. Le moment de la communication en cas d'opération de paiement isolée. – Dans le cas d'une opération de paiement isolée, l'information générale obligatoire prévue à l'article VII.15 du CDE doit être communiquée avant que l'utilisateur ne soit lié par un contrat ou une offre¹⁹¹. Par dérogation, si, à la demande de l'utilisateur de service de paiement, le contrat est conclu par un moyen de communication à distance ne permettant pas au prestataire de communiquer l'information conformément à la phrase précédente, ledit prestataire communiquera ladite information immédiatement après l'exécution de l'opération de paiement¹⁹². Le législateur permet également au prestataire de s'acquitter de son obligation d'information en fournissant un exemplaire

¹⁸⁶ Art. VII.7, § 2, du CDE.

¹⁸⁷ Projet de loi n° 3131/001 précité, p. 23.

¹⁸⁸ Pour les informations à communiquer en cas d'opération de paiement isolée, voy. l'article VII.14, § 1^{er}, alinéa 2, du CDE ; pour les informations à communiquer en cas de contrat-cadre, voy. l'article VII.21, § 1^{er}, alinéa 2, du CDE.

¹⁸⁹ *Ibid.*

¹⁹⁰ *Ibid.*

¹⁹¹ Art. VII.14, § 1^{er}, alinéa 1^{er}, du CDE.

¹⁹² Art. VII.14, § 2, du CDE.

du projet de contrat de service ou d'ordre de paiement¹⁹³. Aucune indication toutefois quant au moment auquel ce projet de contrat doit être communiqué n'est mentionnée. Ni l'exposé des motifs de la loi ni la DSP 2 ne donne davantage d'indications. Un tel flottement peut être problématique pour le prestataire qui, lorsqu'il utilise cette troisième option de communication des informations obligatoires, n'est pas en mesure de savoir avec certitude s'il s'est bien acquitté de son obligation légale d'information, le moment auquel ledit projet de contrat doit être communiqué n'étant pas précisé. La combinaison de l'intitulé de la sous-section concernée du CDE (« Informations *préalables* et conditions »)¹⁹⁴ et de l'expression « projet de contrat » semble indiquer toutefois qu'une telle communication doit avoir lieu avant que le contrat ne soit conclu et exécuté. Nous nous interrogeons dès lors sur l'utilité d'une telle troisième option de communication, dans la mesure où elle nous semble d'ores et déjà englobée par la première option prévue à l'article VII.14, § 1^{er}, du CDE, développée précédemment.

48. Le moment de la communication en cas de contrat-cadre. – Les informations relatives au contrat-cadre doivent être communiquées « bien avant » que l'utilisateur de service de paiement ne soit lié par un contrat-cadre ou une offre¹⁹⁵. Le législateur ne donne pas d'indication précise de temps sur ce qu'il s'agit d'entendre par l'expression « bien avant ». Le législateur belge précise néanmoins qu'« il n'y a consentement réel à l'offre effectuée que si l'utilisateur de services de paiement a disposé du temps nécessaire pour consulter et comprendre les informations et le contrat-cadre avant d'accepter l'offre »¹⁹⁶. Dès lors, on doit comprendre que le prestataire est tenu de laisser à l'utilisateur le temps qui lui est nécessaire pour lire et comprendre l'ensemble des informations qui lui sont fournies au regard du contrat-cadre qu'il envisage de conclure.

En agence, cela signifie que le futur utilisateur doit être mis en situation de pouvoir lire, sereinement, les informations (en ce compris le projet de contrat-cadre envisagé) qui lui sont présentées. À ce titre, le personnel de l'agence et/ou le conseiller devront laisser le temps et l'espace adéquats pour une telle lecture et compréhension, au besoin en reportant à une date ultérieure la signature du contrat-cadre.

¹⁹³ Art. VII.14, § 3, du CDE.

¹⁹⁴ Sous-section 2 de la section 2 « Opérations de paiement isolées » du chapitre 2 « Informations et régissant les opérations de paiement et les contrats-cadre » du livre VII du CDE.

¹⁹⁵ Art. VII.21, § 1^{er}, du CDE.

¹⁹⁶ Projet de loi n° 2179/001 précité, p. 38 ; lors de la transposition de la DSP 1, le législateur belge avait opté pour une expression autre. À la place de « bien avant », il avait opté pour l'expression « en temps utile ». Il est revenu à l'expression « bien avant » issue des deux directives DSP 1 et 2 avec la transposition de la DSP 2 pour que la loi belge corresponde « davantage au texte et à l'objectif de la Directive ». Il n'a pas modifié pour autant l'explication de fond qu'il avait fournie lors de la transposition de la DSP 1, que nous reprenons dans notre raisonnement et qui, à notre sens, reste donc pertinente ; voy. sur ces différents points le projet de loi n° 3131/001 précité, p. 30.

La même exigence est imposée pour le contrat-cadre conclu à distance, par exemple sur internet. Mais, sur internet, comment le prestataire peut-il s'assurer que le futur utilisateur aura bien pris le temps nécessaire pour prendre connaissance et comprendre l'ensemble des informations qui lui sont présentées ? L'utilisateur consciencieux prendra ce temps, *a priori*, sans difficulté, mais l'utilisateur moins prudent pourrait être amené à conclure immédiatement le contrat-cadre, sans s'être accordé le bénéfice d'une lecture sereine des informations et conditions contractuelles que lui propose le prestataire. C'est d'ailleurs un scénario classique en matière de commerce électronique où il faudrait être somme toute assez naïf pour postuler le contraire, peu de personnes lisent, du moins du début jusqu'à la fin, les conditions générales des sites de vente en ligne. Tant pis pour l'utilisateur non prudent, pourrions-nous répondre ? En matière de services de paiement, une telle conclusion est loin d'être évidente. En comparaison avec la réglementation applicable à la vente de biens ou de services (non financiers) en ligne¹⁹⁷, qui n'exige de fourniture de l'information obligatoire qu'« avant » que le consommateur ne soit lié par un contrat à distance, en matière de services de paiement, l'exigence temporelle est plus stricte : l'information doit être fournie « bien avant ». Il nous semble que le prestataire sur qui, on le rappelle, repose la charge de la preuve de l'accomplissement de l'obligation d'information, en ce compris de la communication de cette information « bien avant » que l'utilisateur ne soit lié par un contrat-cadre, doit donc mettre en place des moyens techniques empêchant une acceptation immédiate des conditions contractuelles. Ces moyens techniques pourraient prendre, par exemple, la forme de l'envoi par e-mail desdites informations et conditions, et l'obligation faite à l'utilisateur de renvoyer une confirmation de la bonne réception de cet e-mail, ou d'un parcours de contractualisation en ligne composé d'étapes successives obligatoires, impliquant par exemple une signature électronique, empêchant une acceptation immédiate et irréfléchie par l'utilisateur des informations et conditions.

Si, à la demande de l'utilisateur de service de paiement, le contrat est conclu par un moyen de communication à distance ne permettant pas au prestataire de communiquer l'information conformément aux développements précédents, ledit prestataire communiquera ladite information immédiatement après la conclusion du contrat-cadre¹⁹⁸.

Comme pour les opérations de paiement isolées, il est possible au prestataire de s'acquitter de son obligation d'information en fournissant un exemplaire du projet du contrat-cadre¹⁹⁹.

¹⁹⁷ Sur cette réglementation, voy. en particulier les articles VI.45 et suivants du CDE.

¹⁹⁸ Art. VII.21, § 2, du CDE.

¹⁹⁹ Art. VII.21, § 3, alinéa 1^{er}, du CDE ; sur le moment auquel cet exemplaire de projet de contrat-cadre doit être communiqué, nous renvoyons aux réflexions faites sur ce point dans le cadre des développements sur les opérations de paiement isolées, voy. *supra*, même paragraphe.

L'utilisateur peut par ailleurs demander, à tout moment au cours de la durée contractuelle, de recevoir lesdites informations²⁰⁰.

Enfin, les informations relatives à toute opération de paiement individuelle couverte par le contrat-cadre²⁰¹ sont communiquées à l'utilisateur payeur, à sa demande et préalablement à toute transaction. Après que le montant d'une opération individuelle a été débité (pour l'utilisateur payeur) ou crédité (pour l'utilisateur bénéficiaire), ou après la réception de l'ordre de paiement, le prestataire doit communiquer sans tarder à l'utilisateur les informations, relatives à cette opération²⁰².

La loi prévoit en outre, au regard des opérations individuelles, que ledit contrat doit permettre au payeur de demander que les informations qu'il doit recevoir après que le montant d'une opération de paiement a été débité de son compte, ou après réception d'un ordre de paiement (référence, montant de l'opération, etc.) lui soient communiquées périodiquement, au moins une fois par mois et selon les modalités convenues avec lui²⁰³. Une telle mesure doit permettre à l'utilisateur de suivre raisonnablement ses dépenses²⁰⁴. Une telle communication prendra la forme par exemple d'extraits de compte ou de relevés des opérations liées à une carte de crédit.

Lorsqu'il est bénéficiaire de l'opération, l'utilisateur doit par ailleurs recevoir le même type d'information et a le droit également de recevoir périodiquement ladite information, sur demande et conformément aux modalités convenues au sein du contrat-cadre²⁰⁵.

Le Roi peut décider, par arrêté royal, de rendre une telle communication obligatoire selon les modalités qu'il détermine, et dont la fréquence sera fixée à une fois par mois²⁰⁶. Une telle faculté n'a pas été mise en œuvre à ce jour.

49. Les deux modalités distinctes de communication de l'information : la « fourniture » et la « mise à disposition ». – Les modalités de communication imposées par le livre VII sont graduelles en ce qu'elles impliquent plus ou moins d'efforts à fournir par le prestataire. Autrement dit, sera exigé un rôle plus ou moins actif de la part du prestataire pour communiquer l'information et, de manière proportionnellement inverse, de la part de l'utilisateur pour recevoir cette information et en prendre connaissance. Selon les cas, la loi se contentera d'une *mise à disposition* de l'information ou exigera une *fourniture* de l'information²⁰⁷.

²⁰⁰ Art. VII.23 du CDE.

²⁰¹ Prévues par l'article VI.26 du CDE ; sur le contenu de ces informations, voy. *supra*, section 1, § 3, A, 2, b.

²⁰² Listées aux articles VII.27 et VII.28 du CDE ; sur le contenu de ces informations, voy. *supra*, section 1, § 3, A, 2, b.

²⁰³ Art. VII.27, § 2, du CDE.

²⁰⁴ *Ibid.*

²⁰⁵ Art. VII.28, § 2, du CDE.

²⁰⁶ Art. VII.27, § 3, et VII.28, § 3, du CDE.

²⁰⁷ Voy. sur ces points le projet de loi n° 3131/001 précité, p. 21.

Pour le législateur européen, il s'agissait de « distinguer deux modalités selon lesquelles le prestataire de services de paiement est tenu de fournir les informations : soit le prestataire de services de paiement devrait fournir, c'est-à-dire communiquer activement, les informations au moment opportun, comme requis par la présente directive, sans autre sollicitation de la part de l'utilisateur de services de paiement, soit les informations devraient être mises à la disposition de l'utilisateur de services de paiement, sur la base d'une demande d'informations complémentaires. Dans la seconde situation, l'utilisateur de services de paiement devrait prendre activement des mesures afin d'obtenir les informations, par exemple en adressant une demande explicite au prestataire de services de paiement, en consultant son compte bancaire en ligne ou en introduisant sa carte bancaire dans un appareil imprimant les extraits de comptes bancaires »²⁰⁸.

Ainsi, l'information sera considérée comme *fournie* lorsqu'elle aura été envoyée dans le corps d'un e-mail ou dans une pièce jointe à un e-mail ou dans un courrier envoyé par la voie postale. Le seul effort que l'utilisateur devra accomplir sera d'ouvrir l'e-mail, et sa pièce jointe, ou d'ouvrir l'enveloppe contenant le courrier qui lui est adressé²⁰⁹. L'information sera considérée comme simplement *mise à la disposition* de l'utilisateur lorsqu'elle sera rendue disponible sur son espace personnel disponible sur le site internet du prestataire ou qu'il pourra y accéder, par exemple, en introduisant sa carte bancaire dans l'un des appareils accessibles dans les agences physiques du prestataire et permettant d'imprimer les extraits de comptes bancaires. Dans de telles hypothèses, l'utilisateur devra accomplir certains efforts actifs pour accéder à l'information qui doit être tout de même rendue disponible et accessible par les prestataires de services de paiement²¹⁰.

Les modalités selon lesquelles l'information légale doit être communiquée varient selon que l'on traite d'une opération de paiement isolée ou d'un contrat-cadre et d'opérations individuelles couvertes par ce contrat-cadre.

Le législateur se contente en effet d'une simple *mise à disposition*, pour l'information devant être communiquée avant l'opération de paiement isolée²¹¹. Ce n'est qu'en cas de demande en ce sens par l'utilisateur que le prestataire devra lui *fournir* l'information sur un support durable²¹². Les modalités de communication de l'information à délivrer, à l'utilisateur payeur ou bénéficiaire selon les cas, immédiatement après avoir reçu un ordre de paiement ou exécuté une opération de paiement isolée, sont identiques à celles de la communication de l'information préalable : par principe, le prestataire peut se contenter d'une *mise à disposition*, et ce n'est que sur demande en ce sens formulée par

²⁰⁸ Considérant n° 60 de la DSP 2.

²⁰⁹ Sur la notion de *fourniture*, voy. le projet de loi n° 2179/001 précité, p. 32.

²¹⁰ Sur la notion de *mise à disposition*, voy. le projet de loi n° 2179/001 précité, p. 32.

²¹¹ Art. VII.14, § 1^{er}, alinéa 1^{er}, du CDE.

²¹² Art. VII.14, § 1^{er}, alinéa 2, du CDE.

l'utilisateur qu'il devra lui *fournir* l'information²¹³. L'obligation d'information à communiquer immédiatement après que le prestataire de services d'initiation de paiement a initié un ordre de paiement est encore plus souple en ce qu'elle indique indifféremment qu'une telle information peut être *fournie* à l'utilisateur payeur et, le cas échéant, à l'utilisateur bénéficiaire ou *mise à leur disposition*²¹⁴.

Les modalités de communication de l'information seront bien plus strictes au regard des informations concernant un contrat-cadre. Lesdites informations doivent en effet être *fournies* à l'utilisateur²¹⁵. La possibilité d'une simple *mise à disposition* n'est plus mentionnée. Il en est de même concernant les informations que le prestataire doit communiquer après une opération de paiement individuelle couverte par le contrat-cadre²¹⁶, ainsi que pour les informations à communiquer à la demande de l'utilisateur préalablement à une transaction²¹⁷.

Dans un arrêt *Content Services*²¹⁸, dans lequel était en jeu la directive concernant la protection des consommateurs en matière de contrat à distance²¹⁹, la Cour de justice a eu à connaître d'un site internet permettant de télécharger des logiciels gratuits ou des versions d'essai de logiciels payants. Il était reproché au site internet de Content Services de ne pas *fournir* les informations devant être communiquées au consommateur, et notamment les informations obligatoires concernant le droit de rétractation. Pour pouvoir utiliser ledit site, les internautes devaient remplir un formulaire d'inscription. Lorsqu'ils passaient leur commande, les internautes devaient, en cochant une case, déclarer qu'ils acceptaient les clauses générales de vente et qu'ils renonçaient à leur droit de rétractation. Les internautes pouvaient visualiser les clauses relatives au droit de rétractation en cliquant sur un lien figurant sur la page à remplir pour la conclusion du contrat. Une fois la commande transmise, l'internaute concerné recevait de Content Services un courriel comportant un renvoi à une adresse internet, assorti d'un nom d'utilisateur et d'un mot de passe. Le courriel en question ne comportait aucune information sur le droit de rétractation. Les informations relatives à ce droit de rétractation ne pouvaient être obtenues que par le lien transmis par ledit courriel. La Cour était, dans ces conditions, interrogée sur le point de savoir si le site internet qui se contente de communiquer les informations, dont la directive exige qu'elles soient *fournies* au consommateur, par un lien hypertexte inséré dans un courriel, remplit ou

²¹³ Art. VII.18 et VII.19 du CDE.

²¹⁴ Art. VII.16 du CDE.

²¹⁵ Art. VII.21, § 1^{er}, du CDE.

²¹⁶ Art. VII.27 et VII.28 du CDE.

²¹⁷ Art. VII.26 du CDE.

²¹⁸ C.J., arrêt *Content Services Ltd c. Bundesarbeitskammer*, 5 juillet 2012, C-49/11, EU:C:2012:419 ; pour un commentaire de cette décision, voy. en particulier H. JACQUEMIN, « Arrêt "Content Services" : l'exigence du support durable dans les contrats à distance », *J.D.E.*, 2012/8, n° 192, pp. 243-246.

²¹⁹ Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, *J.O.C.E.*, L 144, 4 juin 1997, abrogée et remplacée depuis par la directive 2011/83 relative aux droits des consommateurs.

non l'exigence de *fourniture* desdites informations. La Cour a répondu par la négative. Pour la Cour, « les termes "recevoir" et "fournies", utilisés à ladite disposition, renvoient à une procédure de transmission, le premier du point de vue du consommateur et le second de celui du fournisseur. Dans le cadre d'une procédure de transmission d'informations, il n'est pas nécessaire que le destinataire de celles-ci effectue une action particulière. En revanche, en cas d'envoi d'un lien au consommateur, ce dernier doit agir pour prendre connaissance des informations en cause et il doit, en tout état de cause, cliquer sur ce lien »²²⁰. Elle a conclu, à ce titre que la « pratique commerciale qui consiste à ne rendre accessibles les informations prévues à cette disposition que par un hyperlien sur un site internet de l'entreprise concernée ne satisfait pas aux exigences de ladite disposition, dès lors que ces informations ne sont ni "fournies" par cette entreprise ni "reçues" par le consommateur »²²¹. Ainsi, un lien hypertexte dans le mail de confirmation d'une commande, en aucun cas, ne pourra satisfaire aux exigences de *fourniture* de l'information imposée par le texte.

La Cour a récemment, dans un arrêt *BAWAG*²²², complété sa jurisprudence. Il s'agissait en l'espèce d'une banque exerçant notamment en ligne sur le marché autrichien. L'une des questions posées à la Cour était la suivante : une information transmise par le prestataire de services de paiement à l'utilisateur de ces services en ligne au moyen d'une boîte aux lettres électronique intégrée à un site internet de banque en ligne peut-elle être considérée comme *fournie* au sens de la directive sur les services de paiement²²³ ? La Cour rappelle que « lorsque la directive 2007/64 prévoit que les informations concernées sont fournies par le prestataire [...], c'est ce prestataire qui doit communiquer ces informations activement »²²⁴. Pour la Cour, il ne saurait, à ce titre, raisonnablement être exigé des utilisateurs « qu'ils consultent d'une façon régulière tous les services de communication électronique auxquels ils ont souscrit »²²⁵. La Cour nuance son propos en ajoutant que lesdites informations seront néanmoins considérées comme étant *fournies* « si une telle transmission est accompagnée d'un comportement actif de ce prestataire destiné à porter à la connaissance de cet utilisateur l'existence et la disponibilité de ces informations sur ledit site ». Ce sera notamment le cas par l'envoi d'un courriel à une adresse mail de l'utilisateur qu'il utilise pour communiquer

²²⁰ C.J., arrêt *Content Services*, 5 juillet 2012, C-49/11, point 33.

²²¹ *Ibid.*, point 52.

²²² C.J., arrêt *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG c. Verein für Konsumenteninformation*, 25 janvier 2017, C-375/15, EU:C:2017:38 ; pour une analyse approfondie de cette décision, voy. notamment F. GEORGES, N. GILLARD, J.-B. HUBIN et H. JACQUEMIN, « Chronique de jurisprudence (2015-2017) », *R.D.T.I.*, 2017, n° 68-69, pp. 29 et s., et G. RUE, « Informations transmises via une boîte e-mail intégrée dans un site Internet de banque en ligne », *B.J.S.*, 2017/581, p. 11.

²²³ À l'époque des faits, la directive applicable était la DSP 1. Toutefois, les notions de *fourniture* et de *mise à disposition* des informations sont reprises à l'identique dans la DSP 2. L'analyse que mène la Cour dans son arrêt *BAWAG* est, à ce titre, parfaitement pertinente également pour interpréter la DSP 2.

²²⁴ C.J., arrêt *BAWAG*, 25 janvier 2017, C-375/15, point 48.

²²⁵ *Ibid.*, point 49.

avec d'autres personnes que la banque et dont les parties ont convenu de l'utilisation comme moyen de communication dans le contrat-cadre²²⁶.

Ces deux arrêts tissent en outre un lien étroit entre l'action de *fournir* les informations exigées par la loi et le support via lequel ces informations devront être fournies, qui devra être un support dit *durable*.

50. Le support de la communication de l'information. – La DSP 2 exige que dans tous les cas mentionnés aux paragraphes précédents où l'information doit être *fournie*, elle le soit sur un support papier ou un autre support durable²²⁷.

Le support durable est défini dans le CDE comme « tout instrument permettant à une personne physique ou morale de stocker des informations qui lui sont adressées personnellement d'une manière lui permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées [...] »²²⁸. La définition consacrée par la directive est en substance la même, même si la formulation diffère légèrement²²⁹. Hervé Jacquemin identifie plus particulièrement trois fonctions que doit nécessairement remplir le support durable : (1) garantir la pérennité de l'information, (2) assurer l'intégrité de l'information, et (3) permettre sa lisibilité et son accessibilité²³⁰. Pour la Cour de justice, « le support durable [...] doit garantir au consommateur, de manière analogue à un support papier, la possession des informations mentionnées à cette disposition pour lui permettre de faire valoir, le cas échéant, ses droits »²³¹.

Le législateur belge a pris la liberté de ne plus mentionner, à côté du support durable, le support papier, alors que la DSP 2 continue de l'indiquer comme possible support de l'information au même titre que le support durable. Le législateur belge explique à cet égard que la définition du support durable consacrée dans le CDE inclut nécessairement le support papier²³². Nul besoin donc, selon le législateur, d'indiquer à côté du support durable le support papier. Il rajoute : « Cependant, il doit être très clair que l'utilisateur du service de paiement, conformément à la Directive, est en droit de demander à

recevoir l'information en version papier s'il préfère ce support à tout autre support durable. »²³³ De manière plus générale, le législateur a harmonisé depuis l'ensemble des notions de support durables présentes dans le CDE pour n'en consacrer plus qu'une, celle de l'article I.1, 15^o²³⁴. Pour le législateur, « l'alternative entre l'écrit et le support durable est redondante. En outre, l'utilisation de l'adjectif "autre" donne à penser que l'écrit est une variété de support durable, ce qui n'est pas correct. En conséquence, cette formulation est modifiée par le présent projet de loi en vue de viser uniquement le support durable »²³⁵.

Le nouvel article I.1, 15^o, précise désormais que peut constituer un support durable « [...] le papier ou, dans l'environnement numérique, un courrier électronique reçu par le destinataire ou un document électronique enregistré sur un dispositif de stockage ou attaché à un courrier électronique reçu par le destinataire ». La DSP 2 donne également des indications concrètes de ce qui peut constituer un support durable. Ainsi, seront des supports durables : « les extraits imprimés par les automates bancaires, les CD-ROM, les DVD et les disques durs d'ordinateurs personnels sur lesquels le courrier électronique peut être stocké, ainsi que les sites internet, à condition que ceux-ci puissent être consultés ultérieurement pendant une période assez longue à des fins d'accès à l'information et à condition que ces sites permettent la reproduction à l'identique des informations stockées »²³⁶. La Cour de justice de l'Union, dans l'arrêt *BAWAG* précité, confirme ce dernier point. Avant d'aborder la question de la « fourniture » de l'information²³⁷, elle s'est interrogée sur le point de savoir si le site internet d'une banque en ligne pouvait constituer un support durable. À cet égard, la Cour a relevé, d'abord, que certains sites internet peuvent être qualifiés de « supports durables ». Dans l'arrêt également précité *Content Services*, la Cour avait conclu que le site web de l'espèce ne constituait pas un support durable en ce qu'il ne ressortait pas du dossier que ledit site permettait au consommateur « de stocker des informations qui lui sont personnellement adressées de manière telle qu'il puisse y accéder et les reproduire telles quelles pendant une durée appropriée en dehors de toute possibilité de modification unilatérale de leur contenu par le vendeur »²³⁸. Ce sera en revanche le cas lorsque le site permettra « à l'utilisateur de services de paiement de stocker les informations qui lui sont personnellement adressées d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période adaptée à leur finalité ainsi que reproduites à l'identique » et que « toute possibilité de modification unilatérale de son

²²⁶ *Ibid.*, points 50 et 51.

²²⁷ Art. 44, § 1^{er}, 51, § 1^{er}, et 53, de la DSP 2.

²²⁸ Art. I.1, 15^o, du CDE.

²²⁹ Voy. l'article 4, 35, de la DSP 2, selon lequel le support durable désigne « tout instrument permettant à l'utilisateur de services de paiement de stocker les informations qui lui sont personnellement adressées d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période adaptée à leur finalité et reproduites à l'identique ».

²³⁰ H. JACQUEMIN, « Sous-section 2 – Application de la théorie des équivalents fonctionnels aux formes de protection de la partie faible », in *Le formalisme contractuel*, Bruxelles, Larcier, 2010, pp. 367-369 ; voy. également sur ces fonctions le projet de loi visant à harmoniser les concepts de signature électronique et de support durable et à lever des obstacles à la conclusion de contrats par voie électronique, exposé des motifs, Doc., Ch., 2017-2018, n° 3153/001, pp. 12 et 13.

²³¹ C.J., arrêt *Content Services*, 5 juillet 2012, C-49/11, point 42.

²³² Projet de loi n° 3131/001 précité, p. 25.

²³³ *Ibid.*, p. 26.

²³⁴ Loi du 20 septembre 2018 visant à harmoniser les concepts de signature électronique et de support durable et à lever des obstacles à la conclusion de contrats par voie électronique, M.B., 10 octobre 2018.

²³⁵ Projet de loi n° 3153/001 précité, p. 17.

²³⁶ Considérant n° 57 de la DSP 2.

²³⁷ Voy. *supra*, même paragraphe.

²³⁸ C.J., arrêt *Content Services*, 5 juillet 2012, C-49/11, point 46.

contenu par le prestataire de services de paiement ou par un autre professionnel auquel la gestion de ce site a été confiée [est] exclue »²³⁹. Le site internet qui reconnaît, par exemple, à chacun de ses utilisateurs un espace personnel via lequel il leur fournira les informations qui leur sont destinées, sans qu'il puisse unilatéralement ni supprimer ni modifier lesdites informations, pourra constituer un support durable²⁴⁰.

51. Conclusion. – Le prestataire de services de paiement se doit donc de porter une attention toute particulière à l'information qu'il fournit ou met à la disposition des utilisateurs de ses services, au contenu de ces informations à l'égard duquel, pour certaines, le prestataire n'a quasiment aucune marge de manœuvre et à la manière dont il doit rédiger et communiquer ces informations. La DSP 2 a confirmé la vision de la première directive et l'a renforcé, en ajoutant encore davantage d'informations à communiquer.

Dans la pratique, il s'agira pour le prestataire de communiquer les informations requises de différentes manières en fonction de l'information traitée. Une telle communication prendra la forme, pour bon nombre des informations visées, de règlement général des opérations ou de conditions générales bancaires, d'un site internet adapté ou d'applications mobiles bancaires, permettant par exemple de gérer son compte ou de faire passer un virement via un smartphone ou une tablette, de brochures d'information, de moyens de communication pendant l'exécution du contrat convenus avec l'utilisateur (courriel, courrier postal, courriel au sein d'un site intégré, relevé d'extraits bancaires, etc.). Si la loi belge du 18 juillet 2019 précitée n'a pas modifié la substance des informations à communiquer, elle en a ajouté un certain nombre. Par conséquent, les prestataires se devaient de modifier leurs contrats en cours ou à venir pour tenir compte de tels ajouts et s'y être conformés pour le 30 décembre 2018²⁴¹.

52. Transition, de l'information à la responsabilisation de l'utilisateur. – Fournir à l'utilisateur ou mettre à sa disposition des informations suffisantes sous une forme accessible, claire et intelligible est un moyen de responsabiliser davantage le prestataire en se montrant transparent vis-à-vis des services qu'il propose, même s'il reste techniquement le seul à les maîtriser. C'est également une manière de donner confiance à l'utilisateur qui dispose ainsi, s'il souhaite s'y référer, d'une information lui rappelant, le cas échéant, qu'il a des droits vis-à-vis de ces services et de l'opérateur qui les propose. L'utilisateur informé sera *a priori* plus conscient des engagements et risques potentiels qu'il prend à contracter avec tel ou tel prestataire pour bénéficier

²³⁹ CJ., arrêt BAWAG, 25 janvier 2017, C-375/15, point 44.

²⁴⁰ Voy. en ce sens le document d'orientation de la DG Justice de la Commission européenne concernant la directive 2011/83 relative aux droits des consommateurs, p. 41, https://ec.europa.eu/info/sites/info/files/crd_guidance_fr.pdf.

²⁴¹ Art. 14 de la loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du CDE, précitée.

d'un ou de plusieurs service(s) donné(s). En d'autres termes, en plus de le protéger, l'information tend à le responsabiliser.

En matière de services de paiement, où le spectre de la fraude n'est jamais très loin, conscientiser et responsabiliser les différents acteurs en jeu, en ce compris l'utilisateur, a paru particulièrement crucial. Nous verrons dans les développements qui suivent que l'information de l'utilisateur est, à cet égard, d'autant plus prégnante qu'il a un rôle important à jouer en matière de sécurité.

Section 2

Les rôles respectifs de l'utilisateur et du prestataire en cas d'opérations de paiement non autorisées

53. La sécurité des services de paiements, enjeu de la DSP 2. – Le législateur précise que « la sûreté et la sécurité des services de paiement sont vitales au bon fonctionnement du marché des services de paiement. Il convient dès lors de protéger de manière adéquate les utilisateurs contre [les risques de sécurité liés aux paiements électroniques] »²⁴². L'objectif primordial est d'éviter que des opérations de paiement impactant les fonds d'utilisateurs ne soient réalisées sans son autorisation, de manière malveillante et frauduleuse. Pour le législateur européen, l'enjeu est de taille, en particulier pour ce qui concerne les paiements électroniques dont les formes et les utilisations n'ont cessé de croître et de se diversifier, entraînant dans leur développement également un accroissement des risques²⁴³.

Garantir la sécurité des services de paiement passe par la mise en place d'obligations particulières pesant sur le prestataire de services de paiement, qui doit mettre en œuvre un certain nombre de mesures techniques. Il verra, en outre, sa responsabilité engagée en cas d'opérations de paiement frauduleuses. Toutefois, tout ne repose pas sur les seules épaules du prestataire. L'utilisateur est également sollicité de manière très précise par la loi et sera sanctionné s'il ne s'y conforme pas.

54. Régime de responsabilités du prestataire et de l'utilisateur. – Le législateur a ainsi mis en place un régime inédit visant à assurer la sécurité des services de paiement, au sein duquel utilisateurs et prestataires de services de paiement se répartissent finement les rôles. La mise en place de ce régime ne date pas de la DSP 2. La DSP 1 l'avait déjà dessiné avec précision. Il est à noter que la loi belge du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds²⁴⁴, bien avant la

²⁴² Considérant n° 7 de la DSP 2.

²⁴³ Considérant n° 3 et 7 de la DSP 2.

²⁴⁴ Loi du 17 juillet 2002 précitée. Cette loi a été abrogée par la loi du 10 décembre 2009 relative aux services de paiement, M.B., 15 janvier 2010. Elle avait transposé, en droit belge, la recommandation de la Commission 97/498/CE du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, J.O.C.E., L 208, 2 août 1997.

première loi sur les services de paiement de 2009, en avait également jeté les bases. La DSP 2, si elle ne crée pas le régime, vient en revanche le consolider, protéger davantage l'utilisateur et confirmer, en les affinant, les principes de répartition des responsabilités des différents acteurs.

§ 1. La délimitation de l'opération non autorisée

A. La distinction de l'opération non autorisée d'autres hypothèses

55. L'obligation incombant au prestataire d'assurer la bonne exécution des opérations de paiement. – De manière générale, et cela paraît logique dans la mesure où il s'agit de sa responsabilité contractuelle première, le prestataire de services de paiement est responsable de la bonne exécution des services qu'il propose. Dans ce sens, il doit garantir la bonne exécution des opérations de paiement autorisées, et donc demandées, par l'utilisateur, et selon les conditions posées aux articles VII.48 et suivants du CDE. À ce titre, le prestataire verra sa responsabilité engagée en cas d'opération non exécutée, mal exécutée ou exécutée tardivement, dans les conditions légales prévues^{245 246}, alors que l'utilisateur aura communiqué un ordre de paiement et des identifiants corrects et se sera conformé au contrat de services de paiement conclu avec le prestataire.

56. La sollicitation du prestataire en cas d'erreur commise par l'utilisateur dans un ordre de paiement. – À l'inverse, le prestataire ne sera pas tenu responsable dans le cas où l'utilisateur lui aura communiqué un ordre de paiement erroné fondé sur des identifiants uniques inexacts²⁴⁷. Dans une telle hypothèse, il n'aura pas à récupérer ou restituer les fonds que lui réclamerait l'utilisateur non diligent. Le législateur belge impose toutefois au prestataire de vérifier « pour autant que cela soit possible techniquement et sans intervention manuelle, si l'identifiant unique est cohérent » et de refuser l'ordre de paiement si tel n'est pas le cas²⁴⁸. La DSP 2 ne laisse pas non plus l'utilisateur démuné dans une telle situation. Elle impose désormais au prestataire du payeur de l'assister dans ses démarches pour récupérer les fonds, ainsi qu'au prestataire du bénéficiaire de coopérer dans l'accomplissement de ces efforts²⁴⁹.

57. L'obligation particulière de remboursement en cas d'opération initiée par ou via le bénéficiaire. – Par ailleurs, le prestataire sera tenu de

²⁴⁵ Voy. à cet égard les articles VII.55/3 et suivants du CDE.

²⁴⁶ L'article VII.29 du CDE prévoit néanmoins que lorsque l'utilisateur n'est pas un consommateur, les parties peuvent décider que les articles VII.55/3 à VII.55/7 ne s'appliqueront pas.

²⁴⁷ Art. VII.55/2, § 2, alinéa 1^{er}, du CDE.

²⁴⁸ Art. VII.55/2, § 1^{er}, alinéa 2, du CDE. Il doit être signalé qu'une telle obligation n'est pas issue de la directive.

²⁴⁹ Ainsi, l'article VII.55/2, § 3, du CDE transposant l'article 88, § 3, oblige le prestataire de paiement du payeur, de s'efforcer « dans la mesure du raisonnable, de récupérer les fonds engagés dans l'opération de paiement » et de fournir au payeur « sur demande écrite, toutes les informations dont il dispose [...] afin que celui-ci puisse introduire un recours devant une juridiction » et le prestataire du bénéficiaire de communiquer « au prestataire de services de paiement du payeur toutes les informations utiles pour récupérer les fonds ».

rembourser l'utilisateur payeur dans l'hypothèse d'une opération de paiement autorisée qui a été exécutée et initiée par ou via le bénéficiaire de l'opération, sous réserve de certaines conditions²⁵⁰, sauf dans le cas où l'utilisateur n'est pas un consommateur²⁵¹. Les hypothèses visées par la notion d'opérations initiées par ou via le bénéficiaire seront, par exemple, le paiement par domiciliation²⁵² ou encore le paiement par carte dans un point de vente²⁵³.

58. L'opération de paiement non autorisée. – Enfin – et c'est l'hypothèse qui occupera les prochains développements –, une autre situation doit être bien distinguée : celle de l'opération non autorisée. Une telle hypothèse renvoie à l'opération qui a été exécutée par le prestataire de services de paiement sans qu'elle n'ait été autorisée par l'utilisateur payeur. Il s'agira, par exemple, d'une fraude subie après un acte d'hameçonnage (ou *phishing*)²⁵⁴ ou d'une opération de paiement réalisée avec une carte bancaire volée à son titulaire.

B. La définition de l'opération non autorisée

59. L'opération de paiement autorisée. – Pour déterminer l'opération qui est « non autorisée », il est utile de se référer à l'opération « autorisée », et donc d'identifier les différents éléments constituant l'autorisation d'une opération de paiement.

Une opération de paiement est réputée autorisée si le payeur a donné son consentement à l'exécution de l'ordre de paiement²⁵⁵. La loi dispose qu'à l'inverse : « En l'absence de consentement, l'opération de paiement est réputée non autorisée »²⁵⁶.

La notion de consentement ne fait pas l'objet d'une définition spécifique dans le cadre du livre VII du CDE. Néanmoins, comme le souligne Julien Sad, de manière classique, le consentement impliquera une volonté libre

²⁵⁰ L'article VII.46, § 1^{er}, du CDE précise que le payeur sera remboursé si les deux conditions suivantes sont remplies : (1) l'autorisation de l'opération de paiement n'indique pas le montant exact de l'opération lorsqu'elle a été donnée, et (2) le montant de l'opération dépasse le montant auquel le payeur peut raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances pertinentes de l'affaire.

²⁵¹ Dans ce cas, les parties peuvent décider de déroger à cette règle, conformément à l'article VII.29 du CDE.

²⁵² La domiciliation désigne, en vertu de l'article I.9, 13^o, du CDE, « un service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur ».

²⁵³ Exemples donnés par le SPF Économie dans sa brochure « La nouvelle législation relative aux services de paiement et l'espace de paiement européen unifié », février 2011, p. 48, <https://economie.fgov.be/sites/default/files/Files/Online/Brochure-nouvelle-legislation-SEPA-2011.pdf>.

²⁵⁴ Le *phishing* (hameçonnage ou filoutage) est une « technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but d'usurper l'identité d'une entreprise, d'un organisme financier ou d'une administration » (définition accessible sur le site de la DG Concurrence, de la consommation et de la répression des fraudes française, www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage).

²⁵⁵ Art. VII.32 du CDE.

²⁵⁶ Art. VII.32, § 2, alinéa 3, du CDE.

et éclairée de la part de son auteur²⁵⁷, en l'espèce, l'utilisateur payeur. Le consentement ne pourra émaner que de l'utilisateur payeur. La loi précise que le consentement pourra néanmoins être donné au prestataire de services de paiement par l'intermédiaire du bénéficiaire ou du prestataire de services d'initiation de paiement²⁵⁸, mais en aucun cas via une autre personne (hors les hypothèses de mandat ou de représentations légales²⁵⁹).

La loi ne prévoit pas les modalités ni l'expression de ce consentement auprès du prestataire. En revanche, elle indique expressément que le prestataire et l'utilisateur doivent convenir, contractuellement, de la forme que doit prendre ce consentement et de la procédure à respecter pour le donner²⁶⁰. Le contrat entre l'utilisateur payeur et le prestataire peut également prévoir que l'opération sera autorisée préalablement ou postérieurement à son exécution²⁶¹.

Pour le cas d'une opération individuelle ou isolée, le consentement ne devient définitif qu'à un certain moment : le moment dit d'irrévocabilité, ou le moment au-delà duquel l'utilisateur payeur ne peut plus révoquer son ordre de paiement²⁶². Il s'agit, sauf exception²⁶³, du moment où l'ordre de paiement est reçu par le prestataire de services de paiement du payeur²⁶⁴. Dans l'hypothèse où le moment de réception ne serait pas un jour ouvrable pour le prestataire, l'ordre est réputé avoir été reçu le jour ouvrable suivant²⁶⁵. De même, le moment d'irrévocabilité est reporté au premier jour ouvrable qui suit. La loi permet, par ailleurs, au prestataire de déterminer une heure au-delà de laquelle tout ordre de paiement sera réputé avoir été reçu le jour ouvrable suivant²⁶⁶. Lorsque le paiement est réalisé via une carte bancaire dans un point de vente physique, l'ordre sera réputé irrévocable après que

²⁵⁷ J. SADO, « Les services de paiement », *op. cit.*, n° 360, p. 285.

²⁵⁸ Art. VII.32, § 2, alinéa 2, du CDE.

²⁵⁹ L'hypothèse de l'employé d'une société autorisant, au nom du dirigeant, des opérations de paiement auprès du prestataire de services de paiement de ladite société, et ayant ainsi un mandat particulier pour ce faire de la part de son supérieur peut, dans certaines circonstances, s'avérer très problématique. Lorsque l'employé est trompé par une tierce personne malveillante, l'opération de paiement devra-t-elle être considérée comme autorisée ? Une telle question renvoie au développement du phénomène que constitue la « fraude au président ». Selon le ministère de l'Intérieur français, la « fraude au président consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre » (définition donnée sur le site www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/L-arnaque-au-president-ou-escroquerie-aux-faux-ordres-de-virement-FOVI). Une étude éclairante de la question du caractère « autorisé » ou non de l'opération de paiement exécutée à la suite d'un acte de « fraude au président » a été menée par G. HENNARD, « Responsabilités de l'utilisateur de services de paiement et du prestataire de services de paiement en cas d'allégation d'opération de paiement non autorisée : l'exemple de la "fraude au président" », in *Actualités en droit commercial et bancaire*, Bruxelles, Larcier, 2017, pp. 293-315.

²⁶⁰ Art. VII.32, § 2, alinéa 1^{er}, et § 4, du CDE.

²⁶¹ Art. VII.32, § 1^{er}, alinéa 2, du CDE.

²⁶² Art. VII.32, § 3, alinéa 1^{er}, du CDE.

²⁶³ Liée à l'intervention d'un prestataire de services d'initiation de paiement, une domiciliation et/ou exception contractuellement prévue.

²⁶⁴ Art. VII.50, alinéa 1^{er}, du CDE.

²⁶⁵ Art. VII.48, § 1^{er}, alinéa 3, du CDE.

²⁶⁶ Art. VII.48, § 1^{er}, alinéa 4, du CDE.

le consentement a été donné au commerçant en insérant, par exemple, dans le terminal de paiement, le code PIN de sa carte²⁶⁷. Les domiciliations sont en revanche « révocables jusqu'à la fin du jour ouvrable qui précède la date de débit convenue pour l'exécution de l'ordre de paiement »²⁶⁸.

L'utilisateur payeur peut donc retirer son consentement à tout moment, pourvu que ce retrait ait lieu avant ledit moment d'irrévocabilité et la réception de l'ordre de paiement par le prestataire²⁶⁹. Lorsque l'autorisation a été donnée pour l'exécution de plusieurs opérations, le consentement pourra être retiré ultérieurement, avec pour effet de rendre toutes les opérations qui seraient exécutées postérieurement à ce retrait non autorisées²⁷⁰. Pour le législateur belge, si la DSP 2 reste muette sur la forme et la procédure à respecter pour exprimer ce retrait, « il va cependant de soi que ces éléments doivent être convenus et communiqués »²⁷¹. Le contrat entre l'utilisateur payeur et son prestataire a ici également une place prépondérante. Il doit être noté, enfin, qu'il peut être dérogé contractuellement à cette possibilité légale laissée à l'utilisateur de retirer son consentement lorsque l'utilisateur n'est pas un consommateur²⁷².

60. L'opération de paiement non autorisée. – En conclusion, l'opération de paiement exécutée par le prestataire sera réputée non autorisée lorsqu'elle n'aura pas recueilli le consentement de l'utilisateur. Deux hypothèses doivent alors être distinguées. Dans une première hypothèse, l'utilisateur aura pu donner, en amont, son consentement à une telle opération, mais l'aura retiré avant le moment d'irrévocabilité. Dans une seconde hypothèse, l'utilisateur n'aura, à aucun moment, donné son consentement.

Cette seconde hypothèse concernera, de manière générale, les cas de fraude de la part de tiers malveillants. Le risque de voir se multiplier ce genre d'opérations non autorisées a poussé le législateur à renforcer le régime existant en matière de sécurité. L'enjeu est de prévenir au maximum la survenance de telles fraudes par la mise en œuvre de mesures particulières incombant

²⁶⁷ Exemple donné par le SPF Économie, dans sa brochure « La nouvelle législation relative aux services de paiement et l'espace de paiement européen unifié », *op. cit.*, p. 37 ; art. VII.50, alinéa 2, du CDE.

²⁶⁸ *Ibid.*, p. 48 ; art. VII.50, alinéa 3, du CDE.

²⁶⁹ Lorsque l'opération de paiement envisagée constitue un contrat conclu à distance portant sur des services financiers à l'égard duquel est reconnu un droit de rétractation de quatorze jours, en vertu de l'article VI.58, § 1^{er}, du CDE, l'articulation de ce moment d'irrévocabilité et du droit de rétractation nous semble délicate à organiser en pratique. En effet, sauf l'hypothèse prévue par l'article VI.58, § 2, 2^o, du CDE de la demande expresse de l'utilisateur que le contrat soit exécuté intégralement avant l'expiration du délai de rétractation, qui emporte la non-application du droit de rétractation, l'on peut s'interroger : comment, une fois le moment d'irrévocabilité passé – et l'ordre de paiement reçu par le prestataire du payeur – un payeur pourrait-il se rétracter d'un contrat portant sur une opération de paiement devenue irrévocable ? Sur le droit de rétractation applicable en matière de contrats à distance portant sur des services financiers, voy. notamment M. VAN HUFFEL, « La Directive 2002/65/CE du 23 septembre 2002 concernant la commercialisation à distance des services financiers auprès des consommateurs », *Euredia*, 2003/3, pp. 371 et s.

²⁷⁰ Art. VII.32, § 3, alinéa 2, du CDE.

²⁷¹ Projet de loi n° 3131/001 précité, p. 38.

²⁷² Art. VII.29 du CDE.

tant au prestataire de services de paiement qu'à l'utilisateur, qui doit ainsi participer à la sécurité des services de paiement qu'il utilise.

§ 2. Le renforcement des responsabilités pesant respectivement sur l'utilisateur et sur le prestataire en termes de sécurité

61. L'accroissement des risques d'opérations non autorisées en particulier sur internet. – Le développement du commerce électronique s'est accompagné ces dix dernières années d'une diversification des techniques de paiement en ligne, mais également d'un accroissement des risques de sécurité, dont les risques de fraude et, à ce titre, d'opérations non autorisées²⁷³.

62. Exemples d'opérations de paiement non autorisées. – Une opération de paiement non autorisée pourra, par exemple, être le résultat de l'utilisation par un fraudeur d'une carte de paiement perdue ou volée ou d'un numéro de carte de crédit usurpé pour des achats en ligne, ou d'un acte de clonage (ou *skimming*) de la carte (lorsque les pistes magnétiques d'une carte sont copiées dans un point de vente physique ou à un distributeur automatique de billets), ou encore d'un acte d'hameçonnage (ou *phishing*) (lorsque les données personnelles, en l'occurrence bancaires, d'une personne sont interceptées, par un fraudeur, par l'intermédiaire, en général, de courriers non sollicités)²⁷⁴.

Ces phénomènes ont rendu nécessaire le réexamen du cadre des services de paiement par la DSP 2²⁷⁵. Il s'agissait de renforcer davantage la sécurité et la sûreté des services de paiement.

A. Les mesures de sécurité incombant au prestataire de services de paiement

1. Le renforcement des mesures techniques de sécurité

63. Le renforcement de la sécurité des services de paiement, objectif de la DSP 2. – De manière générale, la DSP 2 s'est fixé pour objectif de renforcer la sécurité des services de paiement, et en particulier des services de paiement en ligne²⁷⁶.

Auparavant, le prestataire était déjà tenu de mettre en place un système lui permettant de s'assurer que l'ordre de paiement qu'il recevait était bien authentifié²⁷⁷. En d'autres termes, le prestataire devait mettre en place une procédure lui permettant d'être sûr que l'utilisation de l'instrument de paiement à

²⁷³ Considérant n° 7 de la DSP 2.

²⁷⁴ Ces exemples sont extraits de la page du site de la DG Concurrence, de la consommation et de la répression des fraudes française, consacrée à « La fraude à la carte de paiement : quels sont vos droits ? », www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/fraude-a-carte-paiement.

²⁷⁵ Considérant n° 3 et 4 de la DSP 2.

²⁷⁶ Voy. à cet égard notamment le considérant n° 7 de la DSP 2.

²⁷⁷ L'ancien article L.9, 11°, du CDE définissait l'authentification comme la « procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité personnalisés ». Une telle définition a été revue et précisée avec la transposition de la DSP 2.

l'origine de l'ordre de paiement avait été réalisée avec les moyens techniques personnalisés fournis à l'utilisateur par le prestataire. Ce système devait lui permettre de prouver, le cas échéant, que telle opération, pourtant contestée par un utilisateur, a bien été authentifiée, et donc autorisée, conformément au contrat de service de paiement. La charge de la preuve d'une telle authentification lui incombait. Une défaillance en termes de preuve au niveau de l'authentification emportait sa responsabilité pleine et entière à l'égard de l'opération de paiement²⁷⁸.

La Cour d'appel de Versailles avait, par exemple, jugé que ne remplissait pas son obligation de sécurité la banque qui s'était contentée de mettre en place, pour l'accès à leur compte épargne en ligne par ses clients, une procédure d'authentification fondée seulement sur l'introduction d'un identifiant et d'un mot de passe créé par le client²⁷⁹.

La DSP 2 maintient ce régime mais va plus loin, en renforçant davantage les obligations pesant sur le prestataire.

64. La refonte de l'authentification et l'authentification forte du client. – Tout d'abord, il est procédé à une refonte de la notion d'« authentification » et il est créé, en outre, le nouveau concept d'« authentification forte du client ».

L'« authentification » désigne désormais la « procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur de services de paiement »²⁸⁰. La transposition offre également une nouvelle définition, celle des données de sécurité personnalisées. Ces données désignent les « caractéristiques personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification »²⁸¹. La définition ainsi précisée a le mérite de clarifier le but de l'authentification dans le chef du prestataire : celui-ci doit, grâce à l'authentification (et aux procédures et moyens techniques qu'il met en place pour la mettre en œuvre), être en mesure de garantir que, derrière l'ordre de paiement qu'il reçoit, c'est bien l'utilisateur de ses services qui agit.

65. La définition de l'authentification forte du client. – L'« authentification forte du client » va plus loin. Elle est définie comme l'« authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît^[282]), « possession »

²⁷⁸ Ancien article VII.34, § 1°, devenu article VII.42, § 1°, du CDE.

²⁷⁹ C.A. Versailles (fr.), 16^e ch., 18 novembre 2010, n° 09/06634, *Marie-Laure C. épse A. c. Natixis Interépargne*, avec la note de E.A. CAPRIOLI, « Authentification et sécurisation des opérations bancaires », *Comm. Com. électr.*, Paris, LexisNexis, octobre 2011, comm. n° 94.

²⁸⁰ Art. L.9, 11°, du CDE.

²⁸¹ Art. L.9, 33/17°, du CDE.

²⁸² Cela pourra être un mot de passe ou un code PIN ; voy. en ce sens le projet de loi n° 3131/001 précité, p. 11.

(quelque chose que seul l'utilisateur possède^[283]) et "inhérence" (quelque chose que l'utilisateur est^[284]) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification »²⁸⁵.

66. Les cas où l'authentification forte est imposée par la loi. – La procédure d'authentification forte du client n'est toutefois imposée au prestataire de services de paiement que dans certaines hypothèses. Le législateur européen a postulé en effet que certains types de services de paiement présentaient davantage de risques que d'autres, et que les mesures de sécurité se devaient d'être adaptées au niveau de risque associé au service de paiement²⁸⁶. Pour le législateur, les opérations de paiement, par exemple sur support papier ou les ordres de paiement passés par courrier ou par téléphone ne doivent pas nécessairement présenter le même niveau de protection que les services de paiement proposés, par exemple, via internet, qui, eux, doivent faire l'objet d'une attention toute particulière²⁸⁷. Le législateur insiste en effet pour que « la croissance solide des paiements par l'internet et par téléphone mobile [aille] de pair avec un renforcement généralisé des mesures de sécurité. Les services de paiement proposés via l'internet ou d'autres moyens à distance, dont le fonctionnement ne dépend pas de l'endroit où sont physiquement situés le dispositif utilisé pour initier l'opération de paiement ni l'instrument de paiement utilisé, devraient, par conséquent, inclure l'authentification des opérations par des codes dynamiques, afin que l'utilisateur soit à tout moment conscient du montant et du bénéficiaire de l'opération qu'il autorise »²⁸⁸.

En conséquence, la DSP 2 a imposé la mise en place de procédures d'authentification forte dans trois hypothèses : (1) lorsque l'utilisateur payeur accède à son compte de paiement en ligne, (2) lorsqu'il initie une opération de paiement électronique, et (3) lorsqu'il exécute une action grâce à un moyen de communication à distance susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse²⁸⁹. Une telle obligation a été transposée en droit belge, non pas par l'intermédiaire de la loi du 19 juillet 2018, mais par le biais de l'article 47 de la première loi de transposition de la DSP 2, adoptée le 11 mars 2018²⁹⁰.

67. Les normes techniques gouvernant les exigences relatives à l'authentification forte. – La DSP 2 prévoyait, en son article 98, que la

²⁸³ Cela pourra être une carte ou un dispositif générant un code d'authentification, comme par exemple un lecteur de carte bancaire ; voy. en ce sens le projet de loi n° 3131/001 précité, p. 11.

²⁸⁴ Par exemple, il pourra s'agir de l'empreinte digitale de l'utilisateur ou la reconnaissance vocale ; voy. en ce sens le projet de loi n° 3131/001 précité, p. 11.

²⁸⁵ Art. 19, 33/16°, du CDE.

²⁸⁶ Considérant n° 96 de la DSP 2.

²⁸⁷ Considérant n° 95 de la DSP 2.

²⁸⁸ *Ibid.*

²⁸⁹ Considérant n° 97 de la DSP 2.

²⁹⁰ Loi du 11 mars 2018 précitée.

Commission européenne, assistée de l'Agence bancaire européenne, intervienne en vue de fixer dans un acte délégué des normes techniques uniformisées et communes gouvernant les exigences relatives à l'authentification forte du client. L'acte annoncé a été adopté par la Commission le 27 novembre 2017²⁹¹. Comme prévu dans la DSP 2²⁹², les mesures de sécurité relatives à l'authentification forte prévues à l'article 47 de la loi du 11 mars 2018 précitée ne s'appliqueront que dix-huit mois après l'entrée en vigueur des normes techniques adoptées le 27 novembre 2017 et publiées le 13 mars 2018, soit le 14 septembre 2019. Selon Denis Philippe²⁹³, les opérateurs belges procèdent déjà à une authentification forte en matière de paiement électronique, de sorte que l'application de l'article 47 de la loi du 11 mars 2018 et des normes techniques n'impliquera probablement pas de changements radicaux dans la pratique. Une étude approfondie des normes techniques devrait cependant être menée d'ici septembre 2019 pour s'en assurer.

68. La mise en place d'analyse de risques et de notification d'incidents. – De manière plus générale, les articles 50 et suivants de la loi du 11 mars 2018 imposent au prestataire de services de paiement de mettre en place des procédures d'analyse de risques et de sécurité prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés, ainsi que des procédures de notification d'incidents opérationnels ou de sécurité auprès de l'autorité compétente, en l'occurrence en Belgique, la Banque nationale de Belgique.

2. La consolidation des autres obligations de sécurité

69. Les mesures de vérification et de prévention d'une opération de paiement suspecte. – Le nouveau régime prévoit toujours la mise en œuvre, dans certaines circonstances, par le prestataire de services de paiement de mesures lui permettant, lorsqu'il a un doute justifié, de prévenir une opération de paiement qui pourrait s'avérer *in fine* non autorisée²⁹⁴.

L'on a d'ores et déjà évoqué l'obligation pour le prestataire de vérifier, dans la mesure du possible et sans que cela n'implique une intervention manuelle, si l'identifiant unique fourni par l'utilisateur dans son ordre de paiement est cohérent, et de refuser l'ordre de paiement si tel n'est pas le cas²⁹⁵.

²⁹¹ Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication, J.O.U.E., L 69, 13 mars 2018.

²⁹² Art. 115, § 4, de la DSP 2.

²⁹³ D. PHILIPPE, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *op. cit.*, pp. 455-477. Voy. également sur ce point, Commission européenne, « Directive sur les services de paiement ("DSP2") : Normes techniques de réglementation permettant aux consommateurs de bénéficier de paiements électroniques plus sûrs et innovants », fiche d'information, http://europa.eu/rapid/press-release_MEMO-17-4961_fr.htm.

²⁹⁴ L'objectif du présent paragraphe est de fournir un certain nombre d'exemples de mesures qui peuvent être prises par le prestataire pour prévenir une opération non autorisée. À ce titre, il n'a pas la prétention d'être exhaustif.

²⁹⁵ Art. VII.55/2, § 1°, alinéa 2, du CDE ; sur ce point, voy. *supra*, section 2, § 1, A.

Dans le même ordre d'idées, le prestataire est autorisé à prendre l'initiative, sous réserve de l'avoir prévu contractuellement, de bloquer un instrument de paiement pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument ou à la présomption d'une utilisation non autorisée ou frauduleuse dudit instrument de paiement²⁹⁶.

70. La confidentialité des données de sécurité personnalisées et de l'instrument de paiement. – Au-delà de l'initiative du blocage que l'on vient d'évoquer, le prestataire qui émet un instrument de paiement a, par ailleurs, un ensemble d'obligations visant à assurer en amont la sécurité dudit instrument²⁹⁷. Ainsi, il doit garantir la confidentialité des données de sécurité personnalisées²⁹⁸ attribuées et fournies à un utilisateur en lien avec un instrument de paiement. Il doit, en d'autres termes, s'assurer que lesdites données de sécurité personnalisées ne sont accessibles qu'à l'utilisateur autorisé à utiliser l'instrument de paiement²⁹⁹. Il doit s'abstenir, en outre, d'envoyer à l'utilisateur un instrument de paiement que ce dernier n'aurait pas sollicité, sauf dans l'hypothèse du remplacement de l'instrument de paiement³⁰⁰. La loi prévoit que le risque de l'envoi d'un instrument de paiement, ou de tout moyen qui en permet l'utilisation, est supporté par le prestataire³⁰¹. Celui-ci doit donc mettre toutes les précautions en œuvre pour assurer un tel envoi de manière sécurisée et confidentielle.

71. Les mises en place des moyens permettant à l'utilisateur de notifier toute opération suspecte. – Le prestataire, de plus, doit prendre un ensemble de dispositions pour permettre à l'utilisateur de jouer son propre rôle pour assurer la sécurité de l'instrument de paiement qu'il utilise et ainsi d'endosser, le cas échéant, la responsabilité qui est la sienne dans cette utilisation. À ce titre, le prestataire de services de paiement a l'obligation de mettre en place les moyens appropriés permettant à l'utilisateur d'accomplir la notification à laquelle il doit procéder, en vertu de l'article 38, § 1^{er}, du CDE, lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement³⁰².

Le prestataire doit donc mettre en place un système de notification, soit directement, soit via une entité désignée, qui doit être disponible 24 heures sur 24, en vue de permettre à l'utilisateur de procéder à la notification visée, sans délai et à tout moment³⁰³. En Belgique, la société Worldline est l'entité qui a été désignée par une grande partie des prestataires de services

²⁹⁶ Art. VII.37, § 2, du CDE.

²⁹⁷ Voy. à cet égard, l'article VII.39 du CDE.

²⁹⁸ On rappelle que le nouvel article VII.33/17^o du CDE définit les données de sécurité personnalisées de la manière suivante : il s'agit « des caractéristiques personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification ».

²⁹⁹ Art. VII.39, 1^o, du CDE.

³⁰⁰ Art. VII.39, 2^o, du CDE.

³⁰¹ Art. VII.39, 6^o, du CDE.

³⁰² Sur cette notification, voy. *infra*, section 2, § 3, A.

³⁰³ Art. VII.39, 3^o, du CDE ; projet de loi n° 3131/001 précité, p. 41.

de paiements émetteurs de cartes pour assurer le service Card Stop, service disponible par téléphone, 7 jours sur 7 et 24 heures sur 24, pour le blocage des cartes de paiement et autres produits de paiement³⁰⁴, et donc permettre à l'utilisateur de procéder à la notification envisagée.

La possibilité de notifier à tout moment (le plus rapidement possible) l'événement litigieux prend une importance cruciale lorsque l'on sait que le moment de cette notification constitue l'une des clés de la répartition des responsabilités entre l'utilisateur et le prestataire *in fine*³⁰⁵.

L'accès à ce système de notification doit être gratuit³⁰⁶.

Le législateur belge explique que cette gratuité doit impliquer « par exemple que le numéro de téléphone que le titulaire de la carte peut appeler afin de faire bloquer sa carte ne peut pas être un numéro payant qui entraîne des coûts supplémentaires en plus de ce qu'un consommateur devrait payer pour une conversation téléphonique ordinaire à son fournisseur téléphonique »³⁰⁷. Les seuls coûts que le prestataire pourra imputer à l'utilisateur sont, le cas échéant, les coûts de remplacement de l'instrument de paiement. De plus, le prestataire doit permettre à l'utilisateur, sur demande, de disposer des moyens de prouver qu'il a procédé à une notification, et ce pendant dix-huit mois à compter de cette notification³⁰⁸. Une fois que l'utilisateur a procédé à la notification visée précédemment, le prestataire doit empêcher toute utilisation de l'instrument de paiement objet de la notification³⁰⁹.

72. La fourniture d'informations à l'utilisateur comme facteur de sécurité. – Il convient de rappeler enfin que le prestataire participe de la responsabilisation de l'utilisateur à l'égard de l'instrument de paiement qu'il utilise, en lui fournissant les informations développées en première partie de la présente contribution dont la loi lui impose la communication.

Plus le contrat de service de paiement, et en particulier le contrat-cadre, sera clair, lisible, et facile d'accès pour une personne non initiée aux services de paiement (à savoir la plupart des utilisateurs), plus l'utilisateur sera sensibilisé aux risques liés à l'utilisation de son instrument de paiement, et donc responsabilisé. La prévention des risques, et notamment des opérations non autorisées et frauduleuses, souhaitée par le législateur, dépend donc de l'intervention de chaque partie intervenante, chacune dans son rôle.

B. Les mesures de sécurité incombant à l'utilisateur de services de paiement

73. Le respect par l'utilisateur des clauses contractuelles le liant au prestataire. – L'utilisateur est également sollicité dans la sécurité de son

³⁰⁴ Informations extraites du site <https://cardstop.be>.

³⁰⁵ Sur ce point, voy. *infra*, section 2, § 3, C.

³⁰⁶ Art. 70 § 1^{er}, d), de la DSP 2 ; art. VII.39, 4^o, du CDE.

³⁰⁷ Projet de loi n° 3131/001 précité, p. 41.

³⁰⁸ Art. VII.39, 3^o, du CDE.

³⁰⁹ Art. VII.39, 5^o, du CDE.

instrument de paiement et de ses données de sécurité personnalisées qui en permettent son utilisation et l'authentification.

Tout d'abord, si le prestataire est tenu de fournir à l'utilisateur un certain nombre d'informations qui prendront la forme de clauses contractuelles pour la plupart, l'utilisateur doit s'engager à s'y conformer.

Le législateur a ainsi estimé utile de rappeler que l'utilisateur habilité à utiliser un instrument de paiement se doit de se conformer aux conditions régissant l'émission et l'utilisation dudit instrument qui lui auront été communiquées par le prestataire³¹⁰. Le législateur rappelle que, toutefois, ces conditions se doivent d'être objectives, non discriminatoires et proportionnées³¹¹. Il précise que « comme le payeur supportera l'entière responsabilité s'il commet une faute lourde en ne respectant pas une ou plusieurs de ces obligations contractuelles concernant les mesures de sécurité [...], il est important que ces conditions contractuelles concernent des mesures raisonnables et proportionnelles que doit prendre le consommateur moyen afin de garantir la sécurité de l'instrument de paiement et les données personnalisées de sécurité »³¹².

74. L'obligation de diligence et de prudence. – De manière plus générale, l'utilisateur habilité à utiliser un instrument de paiement est tenu à une obligation de diligence et de prudence.

Dès qu'il reçoit l'instrument de paiement qu'il est autorisé à utiliser, il doit prendre toutes les mesures raisonnables afin de préserver la sécurité de son instrument de paiement, ainsi que de ses données de sécurité personnalisées³¹³. Aussi, l'utilisateur « doit éviter de noter son code PIN ou tout autre code sous une forme aisément reconnaissable, et notamment sur l'instrument lui-même ou sur un objet qu'il conserve avec cet instrument. Il ne doit pas communiquer son numéro d'identification personnel à un tiers, etc. »³¹⁴ Nous verrons *infra* que cette obligation générale de prudence prend une signification particulière en cas d'opération non autorisée³¹⁵.

§ 3. Les responsabilités respectives de l'utilisateur et du prestataire en cas d'opérations non autorisées

A. La notification sans délai de l'événement litigieux en lien avec son instrument de paiement par l'utilisateur

75. L'obligation de notification sans délai de tout événement suspect. – On a vu que le prestataire était tenu de mettre en place un système

³¹⁰ Art. VII.38, § 1^{er}, 1^{er}, du CDE.

³¹¹ *Ibid.*

³¹² Projet de loi n° 3131/001 précité, p. 41.

³¹³ Art. VII.38, § 2, du CDE.

³¹⁴ Projet de loi n° 2179/001 précité, p. 61.

³¹⁵ L'utilisateur engagera en particulier sa responsabilité et ne sera pas remboursé en cas de négligence grave à ses obligations et notamment à son obligation de diligence et de prudence ; sur ce point, voy. *infra*, section 2, § 3, C, 2, b.

de notification permettant à l'utilisateur de lui notifier, à tout moment, un événement litigieux qui serait survenu en lien avec son instrument de paiement³¹⁶. Le pendant de cette obligation³¹⁷, pour l'utilisateur, réside en un devoir lui incombant d'informer sans délai son prestataire, ou l'entité que celui-ci lui aura indiquée, dès qu'il a connaissance de toute perte, vol, détournement ou toute utilisation non autorisée de son instrument de paiement³¹⁸. Le moment de cette notification est particulièrement important en tant qu'il est un curseur de la répartition des responsabilités respectives entre le prestataire et l'utilisateur en cas d'opérations de paiement non autorisées³¹⁹.

B. Le remboursement immédiat de l'opération de paiement non autorisée par le prestataire

76. Le principe du remboursement immédiat. – Par principe, en cas d'opération de paiement non autorisée, le prestataire de services de paiement doit en rembourser le montant à l'utilisateur contestant l'opération. Le remboursement doit avoir lieu immédiatement après que le prestataire a eu connaissance de l'opération litigieuse ou après en avoir été informé³²⁰. La DSP 2 a ajouté que le remboursement, en toute hypothèse, doit avoir lieu au plus tard à la fin du jour ouvrable suivant la prise de connaissance ou l'information³²¹.

Le remboursement doit avoir pour effet de remettre le compte anormalement débité dans l'état où il se serait trouvé si l'opération non autorisée n'avait pas eu lieu³²². À ce titre, la DSP 2 a précisé que le prestataire doit faire en sorte que la date de valeur à laquelle le montant a été remboursé ne soit pas postérieure à la date à laquelle le compte a été anormalement débité³²³.

77. La dérogation au remboursement immédiat. – La directive a néanmoins prévu une dérogation à ce principe de remboursement immédiat³²⁴. Désormais, le prestataire peut ne pas rembourser immédiatement la somme en question dans l'hypothèse où il a de bonnes raisons de soupçonner une fraude et qu'il a communiqué ces raisons par écrit au SPF Économie³²⁵.

³¹⁶ Art. VII.39, 3^e, du CDE ; sur ce point, voy. *supra*, section 2, § 2, A, 2.

³¹⁷ Le considérant n° 70 de la DSP 2 précise en particulier que : « Afin de réduire les risques et les conséquences des opérations de paiement non autorisées ou mal exécutées, l'utilisateur de services de paiement devrait informer dès que possible le prestataire de services de paiement de toute contestation relative à des opérations de paiement prétendument non autorisées ou mal exécutées, à condition que le prestataire de services de paiement ait rempli ses obligations d'information au titre de la présente directive. »

³¹⁸ Art. VII.38, § 1^{er}, 2^e, du CDE.

³¹⁹ Sur ce point, voy. *infra*, section 2, § 3, C.

³²⁰ Art. VII.43, § 1^{er}, alinéa 1^{er}, du CDE.

³²¹ Art. 73, § 1^{er}, de la DSP 2 ; art. VII.43, § 1^{er}, alinéa 1^{er}, du CDE.

³²² Art. VII.47, § 1^{er}, alinéa 2, du CDE.

³²³ Art. 73, § 1^{er}, de la DSP 2 ; art. VII.43, § 1^{er}, alinéa 3, du CDE.

³²⁴ Art. 73, § 1^{er}, de la DSP 2.

³²⁵ Art. VII.43, § 1^{er}, alinéa 1^{er}, du CDE.

L'idée est de permettre au prestataire qui a une forte présomption qu'une opération de paiement non autorisée résulte d'un comportement frauduleux de la part de l'utilisateur de mener une enquête dans un délai raisonnable avant de rembourser l'utilisateur³²⁶.

78. Les règles particulières en cas d'opération de paiement initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement. – La loi établit des règles particulières lorsque l'opération de paiement non autorisée a été initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement. Dans une telle hypothèse, c'est le prestataire de services de paiement gestionnaire du compte débité qui aura la responsabilité de procéder au remboursement du montant à l'utilisateur³²⁷. Le prestataire de services d'initiation de paiement qui serait responsable de l'opération litigieuse remboursera, sur demande, immédiatement le prestataire gestionnaire³²⁸.

79. Un principe de remboursement nuancé. – Le remboursement du montant par le prestataire à l'utilisateur ne signifie pas nécessairement que le prestataire supportera l'ensemble ou même une partie des pertes subies à la suite d'une opération de paiement non autorisée³²⁹. La responsabilité de l'utilisateur sera en effet, dans certaines hypothèses, mise en jeu.

C. Le partage de responsabilités entre l'utilisateur et le prestataire en cas d'opération de paiement non autorisée

80. L'importance du moment de la notification. – La notification par l'utilisateur du vol, de la perte, du détournement ou de toute utilisation frauduleuse de son instrument de paiement, prévue à l'article VII.38, § 1^{er}, 2^o, du CDE, constitue le moment clé qui va permettre de répartir les responsabilités respectives entre le prestataire de services de paiement et l'utilisateur. La répartition des responsabilités sera effectivement différente selon que l'opération contestée a eu lieu avant la notification ou après³³⁰.

Le régime de répartition des responsabilités prévu par la loi, et développé ci-dessous, n'est impératif que lorsque l'utilisateur payeur est un consommateur et ne revêt qu'un caractère supplétif dans le cadre d'un contrat conclu avec un non-consommateur³³¹.

1. *Les opérations non autorisées exécutées après la notification*

81. Le prestataire responsable pour le tout. – Après que le vol, la perte ou le détournement de l'instrument de paiement a été notifié au prestataire,

³²⁶ Projet de loi n° 3131/001 précité, p. 43.

³²⁷ Art. VII.43, § 2, alinéa 1^{er}, du CDE.

³²⁸ Art. VII.43, § 2, alinéa 2, du CDE.

³²⁹ Voy. en ce sens J. SADO, « Les services de paiement », *op. cit.*, n° 370, p. 301.

³³⁰ Art. VII.44 du CDE.

³³¹ Art. VII.29 du CDE.

le payeur ne supporte plus aucune perte, même en cas de négligence grave, sauf s'il a agi frauduleusement³³².

Pour minimiser le risque de voir sa responsabilité engagée au titre de l'article VI.44 du CDE, l'utilisateur a donc tout intérêt à notifier le plus vite possible à son prestataire, ou à l'entité que celui-ci lui aura indiquée, l'événement litigieux.

2. *Les opérations non autorisées exécutées avant la notification*

a) *La responsabilité de l'utilisateur à hauteur de 50 euros*

82. La franchise due, le cas échéant, par l'utilisateur. – L'utilisateur payeur supportera à concurrence de 50 euros les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé ou détourné, qui seraient intervenues avant la notification³³³. L'idée est « d'inciter l'utilisateur de services de paiement à signaler sans retard injustifié au prestataire de services de paiement le vol ou la perte d'un instrument de paiement et de limiter ainsi le risque d'opérations de paiement non autorisées »³³⁴.

83. La diminution de la franchise due, le cas échéant, par l'utilisateur. – La DSP 2 a abaissé le plafond de responsabilité du payeur, de 150 euros sous la DSP 1³³⁵ à 50 euros désormais³³⁶. Pour le législateur européen, « un montant de 50 EUR semble adéquat pour garantir un niveau élevé et harmonisé de protection des utilisateurs dans l'Union »³³⁷.

b) *La responsabilité de l'utilisateur pour le tout*

84. Présentation des critères de répartition des responsabilités entre l'utilisateur et le prestataire. – La limitation de responsabilité au bénéfice de l'utilisateur n'est pas applicable, et ce dernier supporte toutes les pertes occasionnées par des opérations de paiement non autorisées : (1) en cas d'agissement frauduleux de sa part, ou (2) s'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article VII.38 du CDE³³⁸. Pour rappel, ces obligations sont au nombre de trois³³⁹ : (1) utiliser l'instrument de paiement conformément aux conditions communiquées par le prestataire³⁴⁰, (2) informer sans délai le prestataire de services de paiement de tout vol, perte, détournement

³³² Art. VII.44, § 3, du CDE.

³³³ Art. VII.44, § 1^{er}, du CDE.

³³⁴ Considérant n° 71 de la DSP 2.

³³⁵ Art. 61, § 1^{er}, de la DSP 1.

³³⁶ Art. 74, § 1^{er}, de la DSP 2.

³³⁷ Considérant n° 71 de la DSP 2.

³³⁸ Art. VII.44, § 1^{er}, alinéa 4, du CDE.

³³⁹ Sur ces obligations, voy. *supra*, section 2, § 2, B et section 2, § 3, A.

³⁴⁰ Art. VII.38, § 1^{er}, 1^o, du CDE.

ou toute utilisation non autorisée de son instrument de paiement³⁴¹, et (3) prendre toutes les mesures raisonnables afin de préserver la sécurité de son instrument de paiement et de ses données de sécurité personnalisées³⁴².

85. La charge de la preuve. – La loi fait peser la charge de la preuve de la fraude de l'utilisateur, ou de son non-respect des obligations de l'article VII.38 du CDE, intentionnel ou à la suite d'une négligence grave, sur le prestataire de services de paiement³⁴³. La loi précise à cet égard que « lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement [...] ne suffit pas nécessairement en tant que telle à prouver que [le payeur] a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article VII.38 »³⁴⁴.

La Cour de cassation française a confirmé, dans cinq arrêts rendus le 18 janvier 2017³⁴⁵, qu'aucune présomption ne pouvait effectivement bénéficier au prestataire dans la recherche de la preuve et dans la démonstration d'une fraude ou d'une négligence grave dans le chef de l'utilisateur payeur, même lorsque des procédures d'authentification forte ont été utilisées pour l'opération non autorisée³⁴⁶. Aussi, la Cour française a rappelé que c'est au prestataire « qu'il incombe [...] de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations ; que cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisées »³⁴⁷. Une telle jurisprudence a à nouveau été confirmée récemment, dans un arrêt du 21 novembre 2018. La Cour française rappelle alors que l'on ne peut déduire l'existence d'une négligence grave uniquement de « l'utilisation effective de l'instrument de paiement ou des données personnelles qui lui sont liées »³⁴⁸.

86. L'acte frauduleux. – Pour cerner la notion d'acte frauduleux, il est utile de se référer, à l'instar de Cédric Alter³⁴⁹, aux travaux préparatoires de l'ancienne loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds³⁵⁰, en ce qu'ils donnaient un

³⁴¹ Art. VII.38, § 1^{er}, 2^o, du CDE.

³⁴² Art. VII.38, § 2, du CDE.

³⁴³ Art. VII.44, § 4, du CDE.

³⁴⁴ Art. VII.42, § 2, du CDE.

³⁴⁵ Cass. fr. (com.), 18 janvier 2017, pourvois n^{os} 15-18.102, 15-18.224, 15-18.466, 15-26.058 et 15-22.783.

³⁴⁶ Pour un commentaire de ces arrêts voy. notamment L.-C. HENRY et M.-L. GUINAMANT, « L'utilisation frauduleuse de la carte bancaire après hameçonnage : la recherche d'un équilibre », *Rec. Dalloz*, 2018, p. 2316.

³⁴⁷ Cass. fr. (com.), 18 janvier 2017, pourvoi n^o 15-18.102.

³⁴⁸ Cass. fr. (com.), 21 novembre 2018, pourvoi n^o 17-18.888.

³⁴⁹ C. ALTER, « Droit bancaire général – Réglementation – Devoirs du banquier – Comptes – Services de paiement », *Rép. not.*, t. IX, Contrats divers, livre 11/1, Bruxelles, Larcier, 2010, n^o 380.

³⁵⁰ Loi du 17 juillet 2002 précitée.

certain nombre d'indications sur ce qui doit être considéré comme étant un acte frauduleux de la part du payeur.

Ainsi, il peut s'agir du fait de donner son instrument de paiement avec le numéro d'identification personnel à un tiers et d'adresser ensuite une notification à la banque, ou encore du fait d'utiliser l'instrument lui-même après sciemment avoir notifié sa perte ou son vol à sa banque³⁵¹.

87. La négligence grave. – La DSP 2 apporte, sur le point de la négligence grave, davantage de précisions que la directive qu'elle a remplacé. Elle annonce que « si la négligence implique un manquement au devoir de diligence, la négligence grave devrait impliquer plus que de la simple négligence et comporter un défaut de vigilance caractérisé, comme le serait le fait de conserver les données utilisées pour autoriser une opération de paiement à côté de l'instrument de paiement, sous une forme aisément accessible et reconnaissable par des tiers »³⁵². En d'autres termes, le simple non-respect des obligations de l'article VII.38 du CDE ne suffira pas à caractériser automatiquement une négligence grave. Un certain degré de gravité devra être constaté.

Le CDE rappelle que chaque cas doit être apprécié *in concreto* : pour déterminer la négligence grave, l'on prendra en compte l'ensemble des circonstances de fait³⁵³.

De manière originale, le CDE donne deux exemples de ce que peut constituer une négligence grave. Aussi, sera considéré comme étant une négligence grave, par exemple, « le fait pour le payeur de noter ses données de sécurité personnalisées, comme son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou un document conservé ou emporté par le payeur avec l'instrument de paiement ». L'autre exemple fourni renvoie au « fait de ne pas avoir notifié au prestataire de services de paiement, ou à l'entité indiquée par celui-ci, la perte ou le vol, dès qu'il en a eu connaissance »³⁵⁴.

La jurisprudence a également apporté de nombreux exemples de ce qui doit être considéré comme une négligence grave, même si on rappellera que chaque cas doit être apprécié en fonction des circonstances de fait précises.

Ainsi, la Cour d'appel de Bruxelles, dans un arrêt du 28 février 2012, a jugé que constitue « une négligence grave le fait d'adopter une attitude qui permet aux tiers d'aisément reconnaître le code secret de la carte bancaire. Il s'en déduit que le titulaire d'une carte fait preuve de négligence grave au sens de cette disposition légale lorsqu'il attribue sa date de naissance ou son année de naissance comme code secret à une carte bancaire qu'il garde sur

³⁵¹ Projet de loi relatif aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, exposé des motifs, Doc., Ch., 2000-2001, n^o 1389/001, pp. 31 et 32.

³⁵² Considérant n^o 72 de la DSP 2.

³⁵³ Art. VII.44, § 4, alinéa 3, du CDE.

³⁵⁴ Art. VII.44, § 4, alinéa 2, du CDE.

lui dans le même sac ou le même portefeuille que ses documents d'identité. En effet, dans ce cas, il sera facile au voleur du sac ou du portefeuille de déduire le code secret des documents d'identité du titulaire »³⁵⁵. Le tribunal de commerce de Mons a, par ailleurs, considéré que l'on peut conclure à une négligence grave lorsque le titulaire d'une carte a introduit son code alors qu'il avait remarqué qu'il était observé par une autre personne³⁵⁶. Il a pu être jugé également que le payeur qui laisse sa carte dans une chambre d'hôtel et ne prend pas soin de la mettre dans un coffre-fort commet une négligence grave au sens de la loi³⁵⁷. Dans le même sens, pour le juge de paix de Bruxelles, « Attendu que, à supposer que la carte de Madame d. B. ait été subtilisée dans sa chambre à Edith Cavell pendant qu'elle subissait un examen ou une intervention, il faut bien admettre que dans ce cas la demanderesse a fait preuve d'une négligence grave au sens de la convention des parties et de la loi ; Que laisser son sac, avec sa carte de crédit, accessible aux tiers dans une chambre d'hôpital dont on est censé s'absenter de temps à autre, est contraire aux règles de sécurité les plus élémentaires »³⁵⁸. La Cour de cassation française a par ailleurs affirmé que l'hypothèse du hameçonnage n'excluait pas automatiquement la négligence grave³⁵⁹.

À l'inverse, il a été considéré que ne constituait pas une négligence grave le fait de conserver sa carte Visa « dans un portefeuille, caché dans la boîte à gants d'un véhicule fermé à clé, stationné sur un parking »³⁶⁰. La Cour d'appel de Bruxelles a notamment jugé que la « constatation que la perte d'un portefeuille peut résulter d'une imprudence de la part du titulaire n'est pas suffisante pour prouver l'existence d'une négligence grave dans son chef »³⁶¹. Dans l'hypothèse où le prestataire parviendrait à prouver une fraude ou une négligence grave dans le chef de l'utilisateur, l'utilisateur sera tenu d'assumer seul l'ensemble des pertes consécutives de l'opération non autorisée.

c) L'exclusion de la responsabilité de l'utilisateur

88. Trois hypothèses d'exclusion de responsabilité de l'utilisateur. – À l'inverse, l'utilisateur ne supportera aucune perte dans trois hypothèses déterminées par le législateur. La DSP 2 apporte des bases nouvelles sur ces points.

89. L'impossible détection de l'acte litigieux. – D'une part, le payeur ne supportera aucune perte dans l'hypothèse où la perte, le vol ou le détournement

« ne pouvait être détecté par le payeur avant le paiement »³⁶². Il s'agira, selon le législateur, de cas de « hacking, phishing des données de sécurité personnalisées ou d'un skimming [...]. Le "détournement" vise donc aussi les cas où les données personnelles de sécurité ont été volées alors que le payeur est toujours en possession de son instrument de paiement (par exemple, dans le cas de "phishing" ou le cas où l'instrument de paiement est cloné) »³⁶³. Dans une telle hypothèse, le payeur ne subira aucune perte, sauf si le prestataire parvient à prouver qu'il a agi frauduleusement.

90. La carence liée au prestataire. – D'autre part, le payeur ne devra assumer aucune responsabilité si la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services paiement ou d'une entité vers laquelle ses activités ont été externalisées³⁶⁴. Il est à noter que la réserve de la fraude n'est, dans cette hypothèse, pas prévue.

91. L'absence d'authentification forte. – En outre, l'utilisateur ne supportera aucune perte, sauf agissement frauduleux de sa part, dans une troisième hypothèse : lorsque le prestataire n'exige pas d'authentification forte³⁶⁵. On a vu que la mise en place de procédures d'authentification forte contribuait à renforcer la sécurité des instruments de paiement et donc des fonds des utilisateurs³⁶⁶. On sait également que pour un certain type d'actions, la mise en place d'une procédure d'authentification forte est rendue obligatoire par la loi³⁶⁷. Ici, on comprend que même si le service de paiement envisagé n'est pas soumis à l'obligation de mettre en place un système d'authentification forte, une opération de paiement non autorisée réalisée sans authentification forte n'emportera aucune responsabilité pour l'utilisateur, sauf si ce dernier a agi frauduleusement. Nous supposons que le législateur suggère indirectement au prestataire la mise en place, dans le maximum de cas, de procédures d'authentification forte.

92. La responsabilité du bénéficiaire ou de son prestataire. – Enfin, la loi prévoit que le bénéficiaire ou son prestataire remboursera le préjudice financier subi par le prestataire de services de paiement du payeur, lorsque l'un ou l'autre n'accepte pas une authentification forte du client. Ainsi, le prestataire de services de paiement du payeur qui aura remboursé immédiatement son utilisateur³⁶⁸ pourra se retourner contre le prestataire de services de paiement du bénéficiaire, voire le bénéficiaire lui-même, pour obtenir réparation. En effet, la loi tient pour responsable le bénéficiaire ou son prestataire du fait de n'avoir pas pris les précautions utiles qu'imposait

³⁵⁵ Bruxelles, 9^e ch, 28 février 2012, RG n° 2010/AR/745, www.juridat.be.

³⁵⁶ Comm. Mons, 28 avril 2011, R.D.C., 7/2013, pp. 598 et s.

³⁵⁷ Bruxelles, 23 juin 2011, D.C.C.R., 2012, pp. 120 et s. avec la note de R. STEENNOT.

³⁵⁸ J.P. Bruxelles, 2^e cant., 7 juillet 2006, *Dr. banc. fin.*, 2007/11, pp. 134 et s.

³⁵⁹ Cass. fr. (com.), 28 mars 2018, pourvoi n° 16-20.018.

³⁶⁰ Bruxelles, 13 septembre 2005, *Dr. banc. fin.*, 2006/11, p. 145, cité dans C. ALTER, « Droit bancaire général – Réglementation – Devoirs du banquier – Comptes – Services de paiement », *op. cit.*, n° 380.

³⁶¹ Bruxelles, 4 octobre 2005, *Dr. banc. fin.*, 2006/3, pp. 145 et s., cité dans C. ALTER, *Droit bancaire général – Réglementation – Devoirs du banquier – Comptes – Services de paiement*, *op. cit.*, n° 380.

³⁶² Art. VII.44, § 1^{er}, alinéa 2, 1^{er}, du CDE.

³⁶³ Projet de loi n° 3131/001 précité, p. 46.

³⁶⁴ Art. VII.44, § 1^{er}, alinéa 2, 2^o, du CDE.

³⁶⁵ Art. VII.44, § 2, alinéa 1^{er}, du CDE.

³⁶⁶ Art. VII.44, § 3, du CDE.

³⁶⁷ Art. 47 de la loi du 11 mars 2018 précitée.

³⁶⁸ Conformément à l'article VII.43, § 1^{er}, du CDE.

l'opération de paiement à l'origine du litige. Le législateur précise que : « Ce § 2 fixe donc les conséquences pour les prestataires de services de paiement du refus de recourir à ce système d'authentification forte du client et donc d'assurer la sécurité nécessaire du service de paiement proposé. Cela couvre également le cas existant sous l'actuel article VII.36, § 1^{er}, dernier alinéa, 1^o. À défaut de sécuriser suffisamment le système de paiement, ils en supportent les conséquences financières en cas d'opérations de paiement non autorisées »³⁶⁹. Ainsi, par exemple, un commerçant en ligne qui n'aura pas mis en place une procédure d'authentification forte pour sécuriser les paiements qui seraient effectués sur son site pourra voir sa responsabilité engagée par le prestataire de services de paiement du payeur en cas d'opération de paiement non autorisée en lien avec un achat effectué sur son site³⁷⁰.

Conclusion

93. Rappel des objectifs de la DSP 2. – La DSP 2 s'est donné pour objectif tant le développement des services de paiement dans le marché intérieur que le renforcement de la confiance des consommateurs dans l'utilisation de ces services, et leur sécurisation nécessairement corrélative.

94. L'utilisateur, acteur des services de paiement. – Dans ce cadre, l'utilisateur de services de paiement s'inscrit comme un acteur à part entière de la sécurité des services de paiement qu'il utilise et des instruments de paiements dont il est titulaire.

Le législateur entend lui permettre de disposer de toutes les informations qu'il estime nécessaires pour qu'il puisse procéder à un choix éclairé. En cela, l'utilisateur bénéficie de la part de son prestataire d'une information *a priori* complète, lisible et intelligible. À ce titre, l'utilisateur, du moins lorsqu'il est un consommateur, fait l'objet d'un cadre protecteur en ce que l'information vient à lui et que cette information et les clauses contractuelles qui vont les retranscrire seront guidées de manière très précise par la loi. Par conséquent, l'utilisateur prend moins le risque d'être en proie à un prestataire qui souhaiterait lui imposer des conditions contractuelles iniques ou abusives. Le cadre ainsi développé tend donc non seulement à une meilleure protection de l'utilisateur, mais également à ses plus grandes conscientisation et responsabilisation face aux défis de sécurité que posent sans cesse et sous des formes toujours plus variées les services de paiement.

³⁶⁹ Projet de loi n° 3131/001 précité, p. 48.

³⁷⁰ Voy. par exemple Bruxelles (9^e ch.), 19 juin 2008, RG 2005/AR/2760, www.juridat.be ; pour un commentaire de cet arrêt, voy. notamment H. CULOT, Y. DE CORDT, H. JACQUEMIN et Th. LÉONARD, *op. cit.*, p. 246, n° 411.

95. Les différents rôles du prestataire de services de paiement. – Le législateur confie au prestataire de services de paiement plusieurs rôles fondamentaux. D'une part, un rôle technique : celui de s'assurer de la bonne exécution des ordres de paiement qu'il reçoit de l'utilisateur de ses services. Un tel rôle exige, de la part des prestataires, des démarches parfois lourdes et coûteuses en vue de garantir la sécurité de leurs services de paiement, via notamment la généralisation des procédures impliquant une authentification forte. Le prestataire doit, à cet égard, sans cesse trouver le point d'équilibre entre la sécurité de ses services et les exigences pratiques du marché, qui visent à toujours plus de rapidité et d'efficacité des services (un utilisateur se détournera effectivement rapidement d'un service de paiement qui serait certes très sécurisé, mais impliquerait des démarches fastidieuses, lourdes et lentes), alors même que ces exigences iront parfois dans un sens contraire à celui de la sécurité.

Le prestataire, par ailleurs, se voit confier le rôle de fournir à l'utilisateur les informations légales ou de les lui mettre à disposition, selon les cas. Ainsi, le législateur mise sur une transmission de l'information à l'utilisateur par le biais, en grande partie, du contrat. L'utilisateur qui accepte d'être lié à un règlement général des opérations, ou autres clauses contractuelles qui lui seraient présentées par un prestataire de services de paiement, pourra moins se cacher derrière une éventuelle ignorance d'une loi trop complexe dès lors qu'il aura, *a priori* en conscience, accepté les informations contenues dans ledit contrat. L'utilisateur s'engageant contractuellement se conscientise et se responsabilise. C'est du moins le postulat qui, selon nous, guide la mise en place du régime décrit dans ces pages.

Encore faudrait-il, toutefois, pour que ce postulat ne reste pas un vœu pieux, que l'utilisateur prenne le temps nécessaire pour comprendre et accepter ces clauses contractuelles. Pour cela, ces clauses devront être rédigées d'une manière qui le lui permette. En d'autres termes, elles ne devront être ni trop longues (on notera que certains règlements bancaires font parfois plusieurs dizaines de pages, et l'ensemble des conditions particulières liées à tel service ou à telle carte, mises bout à bout, peuvent dépasser la centaine de pages) ni trop techniques ou complexes. Il est vrai qu'à cet égard, la loi impose aux prestataires de procéder à un véritable travail d'équilibriste, en ce qu'ils doivent, d'un côté, insérer dans leurs contrats-cadres l'ensemble des informations légales, dont on l'a vu, la liste est longue et l'expression par endroit complexe, et de l'autre, rendre ces informations aussi lisibles et intelligibles que possible pour l'utilisateur moyen non expert en services de paiement. Il reste que des efforts sur ces points nous semblent encore devoir être menés, sans quoi, l'information et la responsabilisation corrélative de l'utilisateur ne resteront, pour partie, qu'illusion.